Privacy requirements of social networking service

Muhammad Farrukh Anwar

University of Tampere
School of Information Sciences
Computer Science / Int. Technology
M.Sc. thesis
Supervisor: Zheying Zhang
June 2016

University of Tampere
School of Information Sciences
Computer Science / Software Development
Forename Surname: Muhammad Farrukh Anwar
M.Sc. thesis, 62 pages, 56 index and appendix pages
June 2016

Users' privacy in the setting of an open internet environment, combined with a social networking environment has increased privacy related vulnerabilities. Privacy vulnerability represents the flaws in an environment or the lack of security from service providers to prevent privacy problems beforehand. Failure to protect user privacy could increase the chances that users' data would be transferred without consent, duplicated, shared or used in an inappropriate context. Social networking services (SNS) mostly rely on user data to operate properly, user data can be provided by user, can be collected from alternate sources, or could be requested by SNS themselves. Data shared by the user may contain personal information, and inappropriate use of that personally identified information (PII) is the main concern in this study.

This study aims at analyzing privacy vulnerabilities in a social media context. The study explores vulnerabilities and privacy policies, and falls in the category of qualitative research. A method to analyze risk imposed by each vulnerability is also discussed at the end of this study. These heuristics are outcome of analysis of various privacy related concepts and privacy taxonomy proposed by Anton (2004). Individual interviews were also carried out to validate findings of this research where developers were asked questions related to privacy vulnerabilities extracted from Facebook privacy policies and other available documents.

The outcome of this research highlights the use of goal based requirement analysis method to evaluate requirements and to determine amount of vulnerabilities related to Facebook and also how the vulnerabilities can be narrowed down. Considering the original study by Anton (2004) was designed for e-commerce websites, some elements had to be modified to suit social networking services where data sharing and data transfer are the core features of the service.

Keywords: Social media, privacy, privacy requirements, privacy vulnerabilities, privacy protection.

Acknowledgements

First of all, I would like to express by deepest gratitude to my supervisor Zheying Zhang, who worked tirelessly to ensure I was on the right path, I would also like to thank her for the continuous support of my masters' thesis, for her patience and immense knowledge in the subject. Your advice on the subject and continuous insight on the progress of my thesis have been priceless.

A special thanks to my family as well, for providing continuous support and motivation throughout the course of my thesis.

Muhammad Farrukh Anwar
June 2016, Tampere

Table of Contents

List of figures

List of tables

1. Introduction

Since their introduction, social networking services (SNS) have attracted millions of users [Boyd and Ellison, 2010]. Providing the ability to be connected everywhere, not only has social media emerged as a platform for communication, but it also has become an important element in our daily lives. Privacy concerns had always been associated with internet usage, because of its nature, personal data on internet can easily be copied and replicated provided the data is not carefully handled [Malhotra et al, 2004].

Due to the nature of social networking services which allows propagation of information, SNS are explicitly targeted [Sullivan, 2011], and rightly so as privacy of users' on such services is often compromised [Boyd and Ellison, 2010]. When there are over 1.3 billion Facebook users alone [Prigg, 2014], it becomes important to evaluate privacy requirements and privacy vulnerabilities of SNS applications.

To highlight privacy vulnerable features, an example can be taken from Facebook Beacon which was launched in 2007. Beacon was designed to advertise to user's friends and connections what a user had purchased recently [Cashmore, 2009]. The feature was then removed from Facebook amid the privacy concerns highlighted by the users [Cashmore, 2009]. Facebook was found to be collecting data with partner sites and as a result a lawsuit was filed against Facebook, for which Facebook had to pay $9.5 million in damages [Cashmore, 2009].

Collecting user information and aggregating it without consent of the user is perhaps the norm of big data web services [Richards and King, 2014]. Combination of powerful communication, extensive and flexible data storage and context aware applications has enabled automated generation and collection of metadata about everything a user does on SNS [Richards and King, 2014]. Such an example can be taken from Facebook, where Facebook gathers facial recognition data based on users' tagged photos without their consent, which perhaps is a grieve privacy vulnerability [Albarran, 2013].

Privacy policies and requirements are quite often similar as the both express a desired state or condition. However, software requirements highlight business goals where as privacy policies iron out the inconsistencies and fill out the gaps between requirements and privacy issues. Many stakeholders participate while highlighting software requirements, privacy of users' may not be their top most concern and privacy and security feature may be developed as an after thought [Liu *et al,* 2003].

1.1 Research Questions

Because of its extensive use and the nature of data associated with social networking services, it is important to understand the techniques used by social networking services to collect, store, process, transfer and retrieve user information. Analysis of such topics

would help to identify potential flaws and workings of SNS along with potential threat each functionality poses on users' privacy.

Analyzing and processing the research questions requires a research methodology and a subject. Facebook with more than 1.3 billion monthly active users [Prigg, 2014] remains one of the most actively used SNS application. Aided by its popularity, privacy values of Facebook and features associated with privacy values would be thoroughly analyzed. For the purpose of analyzing Facebook, the research will investigate and answer following questions.

- How can features impacting on privacy issues be extracted of an existing system?
- How can features be categorized as vulnerable ones?
- How can vulnerabilities be analyzed to determine their severity on users' privacy?

To determine and extract features of Facebook, several documents will be studied such as privacy policy documents, terms and conditions, cookie policies, data storage policies and Facebook graph documentation. Once requirements are elicited, they will be categorized as privacy protection goals or privacy vulnerability goals with help of taxonomy presented by [Anton and Earp, 2004].

1.2 Research methodology

For the research, the main source of information are the research papers, Goal based requirement analysis method [Anton, 1996] and also privacy taxonomy suggested by [Anton and Earp, 2004]. Their research will contribute significantly in evaluating functionalities of Facebook where GBRAM process will provide a list of functionalities in shape of requirements, privacy taxonomy would contribute by identifying privacy related features.

The analysis will yield privacy related features in form of requirements, however, one question remains un answered, how to analyze privacy vulnerabilities and evaluate their severity with respect to end user. T answer this question, an explorative research on privacy taxonomy [Anton and Earp, 2004] and an interview session with a focus group should provide clarity on determining severity of a functionality on an end users' privacy.

The goal based requirement analysis method (GBRAM) process identifies goals, which in current scope and context of social media privacy are more appropriately rephrased as requirements. As all evaluation methods, GBRAM requires a source of input document(s), since vulnerabilities of Facebook are to be determined with respect to end user, Facebooks' data policy [Policy, 2015], selective cookie policy [Cookies, 2015], selective functionalities from Facebook graph API [API, 2015], and selective statement

of rights and responsibilities [Rights, 2015] have been chosen as the inputs. These policies are listed in **Appendix A.**

Facebooks' data policy [Policy, 2015] highlights data management practices such as data collection, data sharing, data usage and data aggregation. These policies define scenarios an end to end user may experience in day to day use. These scenarios should help to identify privacy vulnerabilities related to data management practices and privacy vulnerabilities users' may inflict on themselves on Facebook where data management related vulnerabilities include behavior of a functionality, unnecessary storage of data, indirect data collection and data transfer.

Users actions may sometimes be a cause of privacy vulnerability as well, these range from choosing the wrong combination of privacy settings to the lack of knowledge about the system, third party application usage and the excessive data sharing.

Cookies are small documents placed in users' browser which may hold certain amount of information ranging from the last server activity to users' language preferences [Kristol, 2001]. On Facebook, these cookies are Pixels, which are not only placed when a users' accesses Facebook, but are also used when a user visits a third party service. Understanding what information is stored in a Facebook pixel and how it is used; is important to evaluate privacy vulnerabilities on Facebook.

Developers may also use services of Facebook to access user data and aggregate it to provide new and exciting features to users. These features are often delivered as third party applications. An example of which is Spotify[1], an internet dependent music streaming service on which a user may register themselves using Facebooks' single sign on feature. Spotify would then collect basic user information from Facebook, such as name, age, gender, location and a profile picture. Spotify is only one of many applications accessing user data from Facebook and thus analyzing vulnerabilities of API functionalities is significant.

Some concepts related to privacy may help user to understand behavior of a privacy preserving system, such as right to be forgotten and privacy paradigms. Statement of rights and responsibilities on Facebook highlight what a user can expect from Facebook, analyzing these documents would identify if privacy paradigms are adapted on Facebook. Finally, data types collected by Facebook will also be studied [Data, 2015] which will help to establish categories which users deem are sensitive and more vulnerable to their privacy.

Not all cookie policies, terms and conditions, and data categories could be accommodated in the study. Only those subjects which seem relevant to stakeholders and which highlight data management practices, system functionalities and user activities are

[1] https://www.spotify.com/fi/: Spotify is an online music streaming service.

being considered. It is important to highlight that for current research the stakeholders include end users, developers and the system.

1.3 Thesis outline

The thesis is structured as follows, Chapter 2 discusses data management practices used by social networking services and types of data gathered by Facebook. Chapter 3 describes what sort of privacy concerns are associated with social networking services and various privacy related concepts such as right to be forgotten. Privacy taxonomy which categorizes goals as privacy protection and privacy vulnerability goals is also illustrated in chapter 3 the taxonomy was proposed by Anton and Earp [2004].

Chapter 4 makes use of GBRAM method and defines the steps involved in extracting goals from privacy documents whereas Chapter 5 applies the approach of privacy taxonomy and GBRAM method.

In chapter 5, findings are discussed as well as a methodology is defined to assess privacy vulnerabilities. Individual interviews are also carried out to verify findings from the approach and are discussed in Chapter 5.

The thesis ends with a section of references which were used as a reference to understand various concepts of privacy and appendix lists the goals extracted from privacy policies of Facebook which are also listed and numbered in Appendix A, B and C.

2. Social networking services

As era of online social networking develops and many online services add social features for their users, the definition of social networking keeps broadening [Altshuler *et al*, 2012]. Social networking services and their features usually vary from one to another. For example, Facebook offers social interaction services, in which Facebook allows its users to communicate via messages, allow users' to post on each others walls, and to share comments and exchange contact information, whereas twitter has an information dissemination centric model [LeBlanc, 2011].

In modern day context, SNS can be defined as a web-based service that allows users to construct a public or a semi public profile within a confined system, articulate a list of friends, share and create a connection with common "friends" [Boyd and Ellison, 2010]. The literal definition of networking implies communication between strangers [Boyd and Ellison, 2010]. However, it is important to note that communication with strangers is not a primary nomenclature of modern social networking services. The way users expand their connections is by traversing through a "friends" list of friends and initiating communication and thus networking on different levels [Boyd and Ellison, 2010].

Facebook was initially launched in 2004 by a Harvard student Mark Zuckerberg. Facebook, when it was launched, had a simple feature list, where users in Harvard were allowed to create a private profile and expand their network. At that time Facebook had limited privacy settings where users were allowed to search other users via name, class year and batch and a user could restrict the view of profile to friends only. Facebook with more than 1.3 billion monthly active users [Prigg, 2014] remains the most actively used SNS application.

Facebook allows its users to create an online persona, which may be real or not. Although Facebook strictly requires that one provides real information, there had been many cases of identity theft. A user can register on Facebook like on any other service. When signing up, a user is required to enter name, email/phone number, date of birth and their gender, from there on it is up to the user how they customize their online profile, the functionality of Facebook has evolved since it was launched in 2004 as context of application broadened, Facebook moved from a social networking service for Harvard, to a social networking service for the world.

A user is allowed to make wall posts or status updates, wall posts can include a text description, a photo, video, mood update, and share geo-location with friends or public. There are privacy settings available to make sure that the target audience is what user expects it to be. As a user, one can define a custom privacy where certain "friends" may explicitly be restricted from viewing a post, global privacy, which allows anyone with a Facebook account to view users posts, friends only privacy mode where only users friends are allowed to view the content as well as friends of friend mode where users friend network can also view the updates. Users' may also categories their friends into

various categories. For instance, as a user, one may group family members and restrict a post to just family members or exclude them from the view list.

When a user posts a picture, a video, or a status, he or she can tag other users, where, depending on tagging preferences, user may be required to get approval of friend before tag action is completed. Once tagged, scope of the content is widened to the users' friend and content visibility increases according to friends' privacy.

The search functionality on Facebook is quite extensive as well. As a user, one may search for another user by his/her name, phone number or email address; search for places by name or location and search for events, groups or pages created by other users [Curtiss *et al*, 2013]. A user has the option to restrict other users from searching them, a privacy settings section on Facebook allows you to do so however, it really contradicts with the concept of networking. A list of common terms used on/for Facebook are stated in Table 1.

Terminology	Explanation
App	Abbreviation used for term application, Facebook allows developers to create games and application such as quizzes for the users of Facebook. Popular example includes an arcade game named Candy crush saga.
Comment	A descriptive reply, which may be associated with a picture or a gesture on friends' wall post, a group post, a page post or on a content shared by any other user.
Like	A gesture method used by Facebook to indicate positive feedback.
Friend	A user that you connect with.
Timeline	A collection of users' status updates, post shares or any other activity.
Notification	A tab that notifies a user of an activity on any subscribed user, page, event or group.
Status	A descriptive post which may or may not be accompanied by a video, picture or location made by user.
@	Command used to tag other users on Facebook.

Table 1. Terminologies used on/for Facebook [Data, 2015]

A user can also maintain a page or a group to promote his/her organization, product or create one for general discussion. If a user creates a page or a group, they are deemed administrators of said group. Anything that happens within that group or a page can be controlled by administrators which includes adding/removing users, banning users, creating, deleting and modifying posts and also delete the page or a group itself.

As a page administrator, user is allowed to promote the page. Promotion of content on Facebook is charged and Facebook promotes and brings users to the said post or page. Users like the page or request to join a group (based on privacy settings) to get a feed of

updates. Feeds don't appear automatically on users' timeline though; one has to subscribe to a page or a group to get the feeds.

Another popular feature of Facebook is the Facebook instant messaging. A user may send any other user a "private" message. A private message is only visible between the interacting parties. Instant messaging also allows users to send files to other users, one can also make a voice call or a video call with another user and it is available on all major mobile platforms including Apples' iOS, Google Android and Microsoft windows phone. If allowed by the user, the messenger can also share current location of the user when they send any update.

2.1 Different types of data in social networking services

Data objects on social networking services are collected from various sources. When users sign up on Facebook, he/she provides the initial data containing basic information such as name, email, phone number and address. To create a pleasurable experience, SNS may require users to input more data over time. The service providers may augment the data to provide relevant content to user and their friends. Data categories visible in downloaded archive and Facebook activity log are discussed in section 2.1.1.

2.1.1 Data collected on Facebook

User data on Facebook can be accessed by logging into an account and proceeding to activity log, or alternatively, user data can be downloaded as an archive. The content on either method is identical and merely presented differently. Downloaded information is presented in form of Hypertext Mark-up Language (HTML) which is a mark-up language used to design the layout of web pages. Data objects stored and retrieved via a download tool, the activity log and Facebook graph API are indexed as follows.

Data objects collected and stored when a user signs up on Facebook include collection of basic user data such as name, email, gender, location and phone number which are accessible via activity log on Facebook, downloaded achieve and graph API. Account signup date, activation date and de activation dates are also collected at account signup.

Account login activity would prompt the system to store session information, IP address and hardware information along with location from where Facebook was accessed. This information is usually only accessible when a user downloads archived data, where system may use this information to detect un authorized access. At the time of login, Facebook may also collect users' browsing history on third party services extracted from cookies and use that information to provide relevant advertisements to the user. At the time of login, hardware information such as contacts may also be synchronized and saved into Facebooks' data storage [O'Reilly, 2011].

When a user starts using the application, he/she may create statuses, like objects, upload photos, comment on objects, share other objects, add/delete friends, start or

participate in existing conversation or change profile details. All of the information amongst other is collected by the system and is accessible via a user interface, activity log, downloaded archive and Facebook API. Some information such as payment history and payment methods such as credit/debit card numbers may not be available in the archive and via API.

A user can also engage in purchasing activities on Facebook, where he/she may buy gifts, buy games or promote their content by purchasing advertisement services. The user must provide the credit card/debit card number, billing and shipping address. This information is collected and stored by Facebook when the user makes a purchase.

When a user creates, modifies deletes or reads content, Facebook may collect statistics and aggregated information. Furthermore, when a user is tagged in a post, the picture is stored as a users' photo and the data may be used to perform facial recognition. While using the service, if a user clicks an ad, Facebook may gather statistics about it and provide new relevant advertisements to the user.

This data collected may be used by Facebook to provide other features and services, for instance, a search feature. Facebook graph search allows users to find other users with their name, email, phone number, gender and location. The searches a user makes are also stored along with a timestamp, though this information is only accessible by the system.

Some data may be used for security purposes, such as login activity. If last known location of user is different than the location user accesses Facebook from, Facebook may use this information to prompt user about this activity. This information may also be used to recognize login from public computers and warn users' against saving their credentials on public computers.

If a user deletes a friend from the list, Facebook may store name and profile information of that deleted friend along with time the friend is deleted. Facebook API may be used by developers to access user data, almost all data user creates or shares is available to be accessed via API. How data is read, deleted modified and created by UI, system and third party application is discussed further in section 2.2.

2.2 Read, write, edit and delete

On a typical social networking service, reading an existing file, writing a new file, modifying an existing file and deleting an existing file are four main operations a user, developer or a system may perform. Based on available documentation, Figure 1 is constructed to show stakeholders interaction with Facebook with respect to read, write, edit and delete operations.

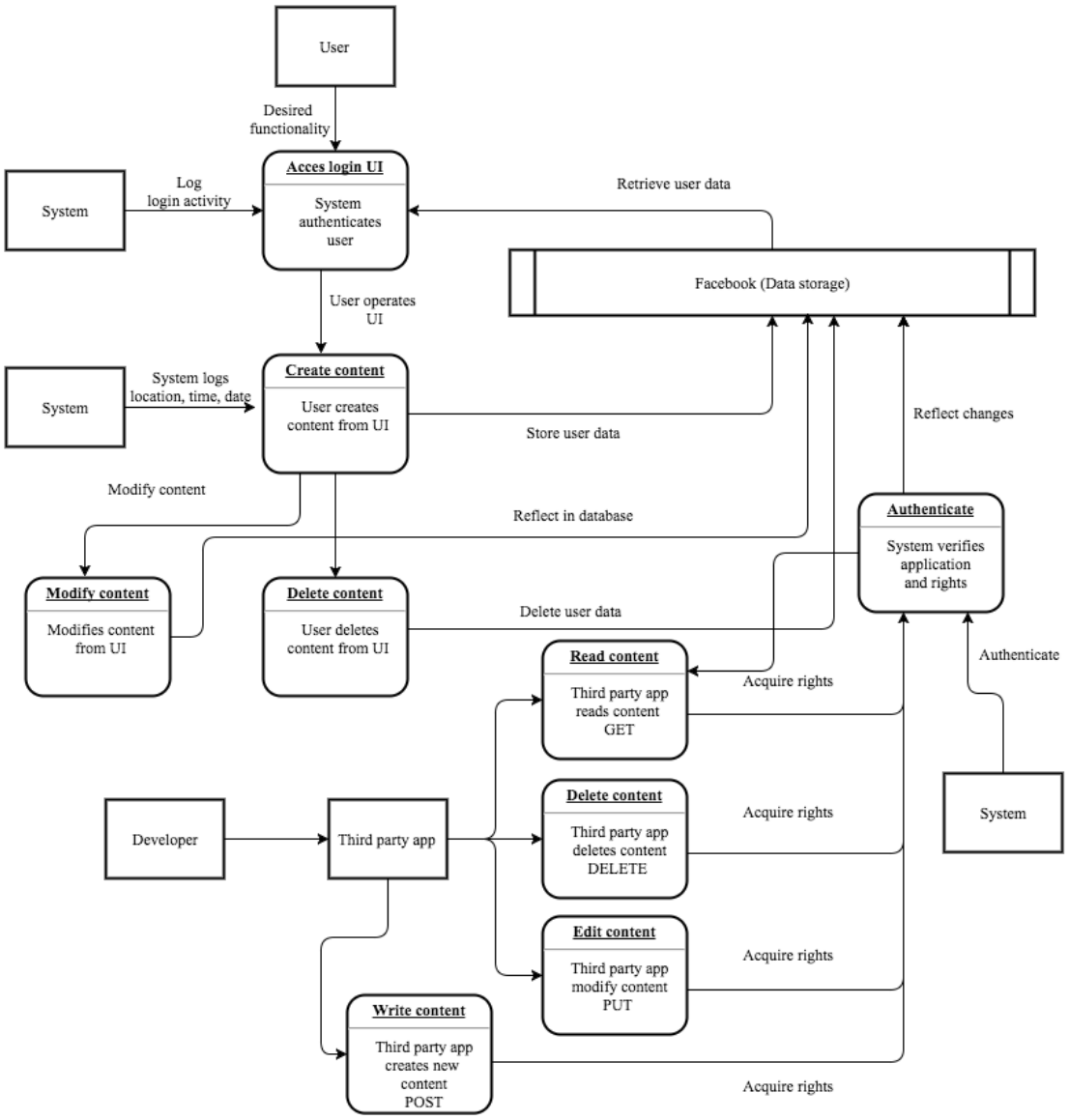

Figure 1. Facebook data operations

As a user, timeline, activity log, and UI can be used to access data from Facebook. A user logs into their account, they get authenticated and data is served to the user. Typically, users are allowed to create, modify, delete and read their content. Some common data categories have been mentioned under section 2.1.1. When a user creates new content, the system logs time and location of created content as well and store it into the database.

Different information may be stored into different data structure, as seen in Table 2. For instance, when a user sends another user a message, it is stored in Hbase and HDFS file format. Hadoop distributed file systems (HDFS) is distributing filing system, which means instructions can be run and computed across many machines in parallel, scalable and size of storage can be increased decreased depending upon the need. The service is fault tolerant and can be run on a standard hardware [Wheeler, 2013]. HDFS by design

replicates data several times, which can be controlled, typically a single copy of data may be replicated three times [Wheeler, 2013], replication ensures faster access to data, its availability and scalability.

	Total Size	Technology	Bottlenecks
Facebook graph	Single petabyte	MySQL and TAO	Random read IOPS
Facebook messages and time series data	Tens of petabytes	Hbase and HDFS	Write IOPS and storage capacity
Facebook photos	>Tens of petabytes	Haystack	Storage capacity
Data warehouse	Hundreds of petabytes	Hive, HDFS and Hadoop	Storage capacity

Table 2. Data storage architecture of Facebook [Borthakur et al, 2011]

Photos and videos a user uploads are stored in a haystack. Haystack has a very general data model that can represent arbitrary pieces of data and metadata and links between them [Adar et al, 1999]. Facebook chooses haystack for photos and videos for its ability to cache content as suggested in Figure 2. For instance, a user has over 800 photos uploaded into their account, the more recent pictures would be cached so that they could be served instantly. However, a lot of requests on Facebook demand older photos, a traditional cache system would fail to serve older pictures, however, haystack has the capacity to handle that information.

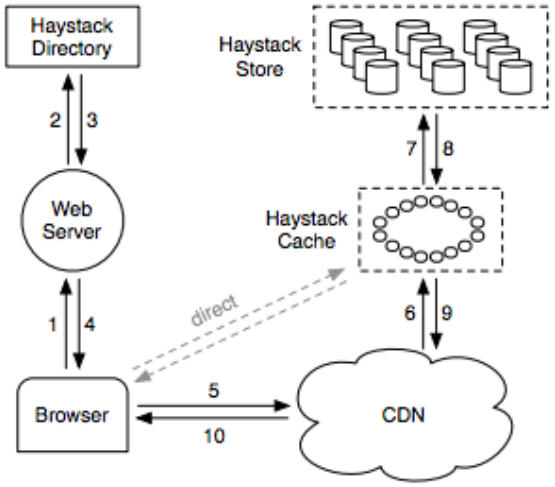

Figure 2. Haystack structure [Beaver *et al*, 2010]

Lastly, all information is also indexed in Facebooks MySQL and the associations and objects (TAO) which is mostly used for Facebook graph API. My structured query language (MySQL) is an open source relational database management system. A typical MySQL database system has tables where tables hold relevant data in rows and columns. A table may consist of several columns; a data type has to be set for a column. Data type

could be an integer, a string, a float, double, character, a variable character, a text or a long text (MySQL n.d.), TAO and MySQL work together to serve trillions of queries. A typical query is illustrated in Figure 3 [Marchukov, 2013].

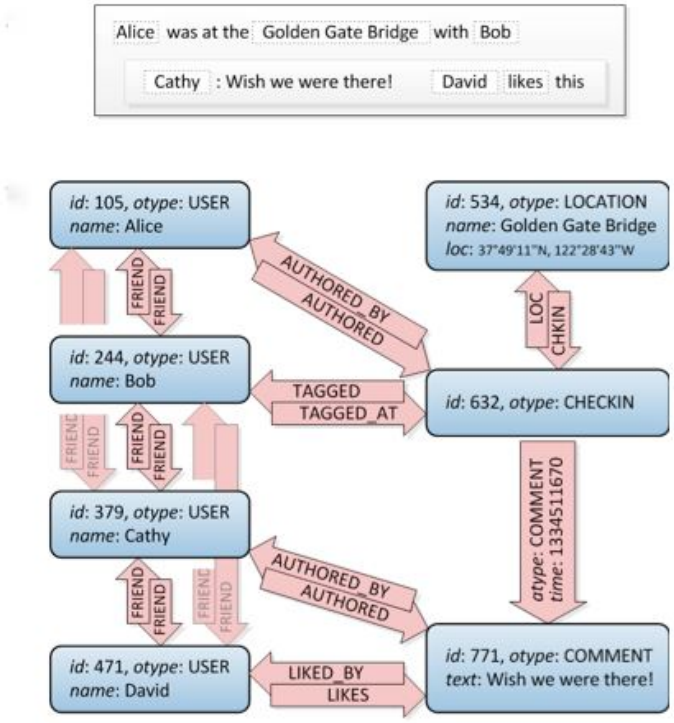

Figure 3. TAO data model and API [Marchukov, 2013]

From illustration represented in Figure 1, it is evident that the user, the system and third party applications have access to user data. When developers develop third party applications, they can access users' public data and once the application is verified, user private data may be accessible as well [Curtiss *et al*, 2013], where Facebook graph API may be used to access use data [O'Reilly, 2011]. Facebook graph API works on principles of HTTP requests, where following methods are allowed to manipulate user data.

- GET: Retrieves content
- PUT: Modifies content
- UPDATE: Modifies content
- DELETE: Deletes content
- POST: Creates content

Figure 3 shows an example where a user Alice checks in at golden gate bridge and user bob is tagged in that check-in. If Bobs' privacy setting is public, then Bobs friend Cathy and Cathy's' friend David may be able to view the check-in as well. It is because of this relationship model that TAO is used for graph API.

It is estimated that from a time period of 2005 to 2020, the overall data storage used globally would reach 400 trillion GB and 5,200 GB of GDSP [Gantz and Reinsel, 2012]. Every week, users contribute up to 260 billion images which takes up around 60 terra

byte of hard disk space [Beaver *et al*, 2010]. Image sharing is perhaps one of the most used feature on Facebook, at a peak time, Facebook may serve up to one million images per second at its peak. Having relational databases and different storage mechanisms for different types of data improves accessibility and data processing speed, however, this results in data duplication and erasure of data upon user command may not be guaranteed.

2.2.1 Data collection

Data collection on social networking services begin when users sign up to the service. Facebook for instance at the time of sign up requires user to fill out a form which includes a name, email address, phone number, date of birth and gender. Once a profile is created, user may provide other information such as high school information, sexual preference, profile picture, things a user likes etc. This data helps social networking services to generate more relevant content and advertisements. The data also helps SNS to provide user with networking suggestions.

Facebook may also collect information that is shared about the user. For instance, a tagged video, a status tag, a tagged photo, check-in, which also store location and time and messages that you send or others may send to you. An example is illustrated in Figure 3, which shows a user Alice was at golden gate bridge and she tagged Bob, where bob is now data owner of that check-in as well.

Facebook may also synchronize address book that a user may have on their device, which includes a personal computer, a cellular device or a tablet PC. Facebook may also synchronize photos a user has on his/her device[2]. Payment details are also collected by most SNS if the feature is available. For instance, advertisement payments can be made on Facebook and they (Facebook) may collect users' credit/debit card information, shipping address, time of purchase and shipping address as well[3].

Device information of user may be collected by social networking services. For instance, as observed in section 2.1.1 (data collected on Facebook), facebook collects name of device[4], IP address of the device, cookie session, geographical location, mobile operator, battery, software, language and time zone [Data, 2015]. Applications that use Facebook social media plugins may monitor data usage of a user and may report to Facebook. Facebook will store that information. This information may be used for displaying relevant advertisements on users' profile page.

Any company that is associated with SNS provider may also collect and store information [Johnson *et al*, 2012]. Facebook owns several popular applications which

---

[2]http://www.digitaltrends.com/opinion/friends-dont-let-friends-use-facebook-photo-sync-privacy-and-data-ownership-issues/

[3] https://www.facebook.com/policy.php

[4] If a user assigns a name to the device, e.g. XYZ-PC

have millions of monthly active users. Application which includes a popular instant messaging application WhatsApp Messenger, a photo sharing application Instagram and a virtual reality gadget, Oculus Rift. Data that is collected on these services may be subjected to collection and monitoring by Facebook.

2.2.2 Data generation

Before data generation techniques and practices are studied, an overview of "business model" is required. Rappa [2003] Defines the business model as "the method of doing business by which a company can sustain itself" and divides business models into categories, such as brokerage, advertisement, infomediary, merchant, manufacturer, affiliate, community, subscription and utility. The category Facebook fits in is undoubtedly "advertisement". In case of Facebook, the website itself provides a platform for advertisers to post relevant content on user profiles. Relation between data generation and advertisements is coherent, and so to generate more revenue, service provider must provide more relevant content to advertisers by aggregating user information. Facebook may use following information to generate new data for advertisers.

- **Location:** Facebook is context aware service, which means that service is aware of what device a user uses to communicate with server, from where the communication originates and/or what action prompted the request. If a user travels, location based advertisements may be prompted on users' device. For instance, a user X travels to Barcelona, then Facebook may provide advertisements of restaurants in Barcelona [Data, 2015].
- **Likes:** User is allowed to "Like" posts, comments, statuses and pages. Facebook aggregates that information with other information like gender, location and email to provide relevant advertisements and sponsored pages. Likes provide an insight for Facebook to understand user behavior and is used to automate advertisement placement.
- **Cookies:** Cookies are small files placed in users' browser which store information such as URL of page accessed, time and location [Acar *et al*, 2015]. Cookies are ideal for monitoring usage of websites as they are really small in size, often referred to as "pixels" and are quick to read by browsers. As a user, most of web services require you to read and accept cookie policy which explicitly defines how a service may use cookies to improve the service. Services like Facebook use cookies to aggregate data and generate content[5]. For instance, if a user queries Google search for "soccer", then

[5] https://www.facebook.com/help/cookies/

Facebook may use that cookie to post advertisements on your page related to soccer [Acar *et al*, 2015].

2.3 Data use and data transfer

Most of social networking services are data driven [Traverso, 2013]. Data that user inputs along with data that is aggregated is used by SNS provider to earn revenue[6]. In most social networking services for example Facebook, it is mentioned in their data policy that service may use data to provide better and relevant advertisements to the user. Apart from advertisements, SNS may also use user data to improve user experience on the service. For instance, Facebook may use the users' data from posts, pages, groups or tagged content to suggest new connections, groups, pages or activities and events taking place near the user. Facebook friend suggestion for instance finds a commonality between user A and user B. Several attributes like work, experience, education, location and mutual friends may be used to suggest new connections. Facebook mobile applications have a limited access to users' mobile device, data such as contact information may be collected and used to suggest networks already existing on vastly popular SNS.

Social networking services may own other services, which means that data from both services can be combined to generate new content, such is a case with Facebook and Instagram. In April 2012, the social networking giant gained right of Instagram[7], as it states on Facebook privacy policy document [Policy, 2015], Facebook has the right to user data found on partner or owned companies, hence pictures shared on Instagram by a user may be used by Facebook. One use can be to improve Facebooks facial recognition system which automatically suggests friends who appear in a certain image.

Data transfer may initiate for several reasons, such as in case of Facebook, the company is based in United States[8], since most of Facebooks data warehouses are based in United States, transfer of data across border may often happen. Some statistical insights may also be shared to partner advertising companies, though, SNS usually removes any personal data[9] from data set before transmission, and these insights provide an overview of an advert out reach.

2.4 Data control

While knowing how and if the personal data are protected; it is also important to know how the data are being used and where they are used. It is also important that the user has

---

[6] https://www.quora.com/How-does-Facebook-make-money

[7] http://www.forbes.com/sites/bruceupbin/2012/04/09/facebook-buys-instagram-for-1-billion-wheres-the-revenue/

[8] https://en.wikipedia.org/wiki/Facebook

[9] Personal data refers to any data that can identify a user

full control of the data put online. Facebook allows a user to disable his/her account, but that does not mean that the data of the disabled account is erased as well. If a user chose to come back, he/she will start from where he/she left. Another flaw is the concept of caching. Consider the scenario: A user logs into his/her social media account through an unknown computer, the user browses for a while and signs out. A computer literate person might be clever enough to erase all traces, but, those who do not know can have their data in the browsers cache. While certain SNS applications like Facebook verifies if it is users' system and asks to save browser (which indeed is a good step) other SNS applications might not do that and the information can fall into wrong hands?

Having a system that gives the user's the ability to upload and post content whilst having the desire to control the information is a challenge of this decade. Perhaps, having both is irreconcilable [Edwards and Brown, 2009]. A typical SNS profile of a user may include their picture, age, sex, location, educational history, marital status and perhaps a few personal wall posts as well (which perhaps were made public). As an SNS user, anyone can go and search a random name and gather some sort of information about a person, such as the person's age, location, where they study, who they are friends with and in this case even life events of the said person.

Although Facebook allows users to control what information is displayed to public, the user has to set the settings up. According to one of the privacy paradigms which are discussed in section 3.1, a user should not be doing that and it must be a "Default measure". There are tons of privacy settings available on Facebook, which indeed is a good thing, but not everyone is aware of them.

3. Privacy and privacy threats in social networking services

It is important to highlight correlation between trust and social networking service usage. Establishing trust with the users so that they would continue to use the application and share the data is essential for SNS [Volakis, 2011]. After all, business model of most SNS applications rely on user's data for ads and other third party services. Trust, as defined by Mayer *et al* [1995, p.712] is "Willingness of a party to be vulnerable to the actions of another party based on the expectations that the others will perform a particular action important to the trustee, irrespective of the ability to monitor and control the other party". In case of social media applications, users are trusting the service with their data without having the control over location of the data they share, whereas the provider is accepting the responsibility of the data exposing themselves to vulnerabilities [Volakis, 2011].

Privacy is a concept that affects the users' interests as opposed to the providers [Cottrill, 2014]. Privacy within an SNS application may not always be expected [Dwyer *et al*, 2007] because of the "social" aspect of the application. For a user to be social over the internet, it is important to provide information, which sometime can be personal information. Unlike face to face communication where a user can choose and also refrain from giving out some information, with internet once the information is shared, it can and will be accessed by unknown readers. Based on the volatile nature of the internet, the importance of privacy is immense; therefore, privacy and its requirements must be analyzed with respect to social networking services.

3.1 Privacy and concepts related to privacy

As defined by Westin [2003] privacy is

> "The claim of individuals...to determine for themselves when, how and to what extent information about them is communicated to others."

The definition of privacy may have different meanings in different environments. For instance, personal pictures shared on Facebook may be considered private but on Instagram sharing pictures is the core functionality. On the other hand, McFarland [2012] defines privacy as a state of freedom where there is no intrusion or interference and as a user, right to be anonymous. Despite different definitions the general concept remains the same.

Privacy plays a fundamental role in human rights policy as well, as stated in Article 8 of the 1950 European convention of human rights[10], privacy has two key elements.

- The right to be left alone.

[10] http://www.echr.coe.int/Documents/Convention_ENG.pdf European convention of human rights

- The right to control what information is shared of oneself.

While the right to be left alone emphasize on confidentiality, the latter suggests that the user must be able to control the information shared about them. If a user does not want certain information on the web, he/she has the right to delete the information for ever.

Facebook collect, share, transfer and uses user data. These processes are carried out by agents. As illustrated in Figure 1, there are three agents who are mainly responsible for manipulating data on Facebook. Agents may have varying responsibilities, which include generating data, collecting data and storing data. When a user provides a name, an email address, a phone number, pictures and an address, the system stores the information in an appropriate database. In this instance, users are agent when they provide information and system is an agent when they process personal data.

Processing of personal data may refer to any information which goes through a process, such as collection, aggregation, retrieval, transfer and usage [Abril and Lipton, 2014]. The process maybe automated such as data aggregation or may be invoked by the user such as information collection. In the example mentioned above, the system is responsible for storing data provided by a user in an appropriate database and the process is personal data processing.

Personal data filing systems are responsible for creating conditions for limiting the view of the user data, whereas controllers are the agents responsible for processing user information [Abril and Lipton, 2014].

A processor is an agent that processes the personal information on behalf of a controller which may be authority, the user, SNS provider or legal agent [Abril and Lipton, 2014]. Third party refers to processing of any personal information by an agent other than legal authority, user, SNS provider who under the authority of controller are allowed to process the data.

Recipient refers to the person to whom information is disclosed to. As illustrated in Figure 1, recipients of information on Facebook may include a user, a system or a developer accessing data through a third party application. Consent refers to an action that validates a controller and a processor to process personal data. Essentially, the data owner gives authority for his/her data to be processed.

Apart from privacy, confidentiality is another key concept in social networking services. While privacy affects the user directly, confidentiality affects the user indirectly since it involves practices SNS provider applies to protect user privacy. These practices involve user data protection techniques, user data usage policies, user data authorization and access, data security, transparency of organizational data management and prevention of malicious attack and access of user data to third party organizations.

3.1.1 Privacy paradigms

Social networking services are developed to provide users a platform to expand their network. In an attempt to make communication more enjoyable, SNS providers may use information from users' device to provide relevant content. According to CISCO systems, 11 billion devices were connected to one another by 2013, the number is estimated to increase to 200 billion devices by the year 2022 [Polonetsky, 2013].

Information security measures and practices constantly need to evolve with time. Privacy by design emphasize the use of proactive measures rather than reactive measures [Cavoukian and Chanliau, 2013]. The paradigm of privacy is based on 7 concepts, which are described below [Cavoukian and Chanliau, 2013].

- *Proactive than Reactive:* The concept believes that privacy should never be left to be handled later. It must always be taken into account before anything is actually developed.
- *A default measure:* The user must not have to change settings of their data to make it private, it should be ensured that most secure privacy settings are applied by default allowing users to change the settings as they wish thus giving control to the user over their data.
- *Incorporated in the design:* The concept of privacy must not come as an added feature. It should be a part of the system: Requirements engineering process takes privacy into account, but not in as much detail as it is required in the "internet of things".
- *Privacy as a feature and not as a compensation:* A service must incorporate all aspects of privacy requirements. Privacy must not be traded off with another feature. For example, privacy may not be compensated for the sake of security. It is better to create a win-win situation for the user than a tradeoff.
- *End to end security:* The concept suggests that if privacy requirements are embedded from the design phase, and before any information is pushed, then the information stored will have the same extend of security from start till the user deletes the information.
- *Transparency of information:* The objective of this concept is to give all stakeholders a retrospective of how information is managed and how it will be managed in case a new feature is implemented. Many new features that make their way to Facebook face a backlash from the users as according to them, it does the opposite of that. However, the SNS provider is not to be completely blamed for that. Users tend to skip privacy policies and long data control statements, perhaps there needs to be a better way of delivering the policies to the users.
- *Respect for user data and privacy:* The software architects, requirement engineers, and stakeholders must all think of users' data and its privacy before

enlisting requirements, developing hardware, developing software and publishing or before using users' content for a new feature or say for advertising.

Privacy by design (PBD) gives a brief yet essential overview of the concept of privacy and how it is expected to be. Social networking services and other platforms that make use of user data must respect user privacy and assure privacy is compliant on all platforms. Apart from above mentioned privacy paradigms, service providers must be held accountable in case of information disclosure, must provide measures to avoid such scenario, assure data integrity and must only collect information when it is necessary [Cavoukian and Chanliau, 2013].

3.1.2 Right to be forgotten

Right to be forgotten is a concept turned law giving people the authority to contest existence of information which a user deems private or if it is invading his or her privacy [Bennett, 2012]. Right to be forgotten comes with a few conditions. The data owner can contest if information provided by any search engine or network is inaccurate, inadequate, irrelevant, or excessive [Bennett, 2012].

According to the EU law on right to be forgotten, the data subject has the right to demand erasure of data at the source and also obtain confirmation of erasure of data from all third party sources and duplicated cases [Bennett, 2012]. To ensure user data are readily available, most providers make several copies of data. In case one origin fails, the backup would supply SNS with information. As established earlier, private information is any information that could link back to data owner and reveal his or her identity. However, right to be forgotten opens up a question whether the law is applicable on data which may indirectly reveal user identity via probability and not certainty [Bennett, 2012]. Information that fits under this category may include photos, text from a conversation, likes and hobbies to name a few and whether it applies to information derived from aggregation.

As it seems from the law, a user has complete control of his or her information, but it may also depend on whether the originating source or platform was public or private. While the right to be forgotten assures erasure of such information, there are a few challenges associated with it as well. The limitations are listed below (Enisa).

- In the world of big data[11], allowing a person to identify and locate all related items stored about them, where several copies may exist.

[11] **Big data** is a broad term for **data** sets so **large** or complex that traditional **data** processing applications are inadequate. Challenges include analysis, capture, **data** cu ration, search, sharing, storage, transfer, visualization, and information privacy.

- Determining locations of all copies of user information.
- Determining whether user holds the right to contest information retention.
- Assurance of erasure of data from all sources.

Out of these limitations, assurance of erasure of data is perhaps the most complicated aspect of right to be forgotten for several reasons. One being duplication and the other, storage of data on offline devices such as backup data hardware, user flash devices and old communication devices.

3.2 Privacy threats in Facebook

Data sharing on social networking services is the core feature and business model for most services. Perhaps, it is the most vulnerable feature as well as it poses severe threats to users' privacy. Users on social networking services can and will share information to expand their network, most of this information will be private for example, work history, education, place of birth, name age, gender, phone number, pictures, statuses, hobbies, comments, statuses and videos to name a few. This information on users' public or semi-public profile can expose a user to identity theft and other privacy issues.

Most social networking services have a solution for enhancing privacy and limiting external visibility. In Facebook, they are called privacy settings. However, these settings are not set as default and the user has to specify these explicitly. Furthermore, this functionality contradicts one of paradigms of privacy that is "privacy by design" which suggests that users should not have to set or improve privacy rather it should be the default feature. Risks associated with a public profile are grave and the default settings can cause various privacy concerns.

A public or even a semi public profile can be indexed by most search engines [Gross *et al*, 2005]. Facebook gives its users the control to stop search engines from indexing their profiles. However, the feature is rather complicated to set. Furthermore, if a user makes a comment, or performs activity on a group[12] or page, that will be indexed on search engines and users cannot affect the settings of such activity[13]. This can leave a massive digital footprint of a user [Gross *et al*, 2005], where a user may choose insecure privacy settings and have all of their information being shared publically.

Whatever users share on social networking service, it can be copied by another network and duplicated countless times. Furthermore, user may not have control over incidental data sharing. Incidental data sharing includes tagging friends in a picture, status or a comment, and comments or activity on other users' wall or shared content. This

[12] A facebook group allows users to socialize in a forum type of structure

[13] https://www.facebook.com/help/186212491428940

activity promotes information leakage [Gross *et al*, 2005] and user may no longer have control over shared information.

Public nature of the data on social networking services also promotes the possibility of trend monitoring, which can easily be misused [Cvijikj and Michahelles, 2011]. The information can be used to determine trends and habits of a user. For instance, if a user likes football, and regularly posts statuses about football, then Facebook might use this information to provide advertisements related to football or notify the user about footballing events happening nearby [Cvijikj and Michahelles, 2011].

Data aggregation helps SNS provide new and relevant content to its users to keep environment exciting for the user. The associations and objects (**TAO**) is a relational data implementation by Facebook [Marchukov, 2013] which serves thousands of calls every day. Facebook API also utilizes TAO which makes it easier for developers to create new applications. Relational data works on the principle of data aggregation. A simple aggregation operation is be visualized in Figure 4.

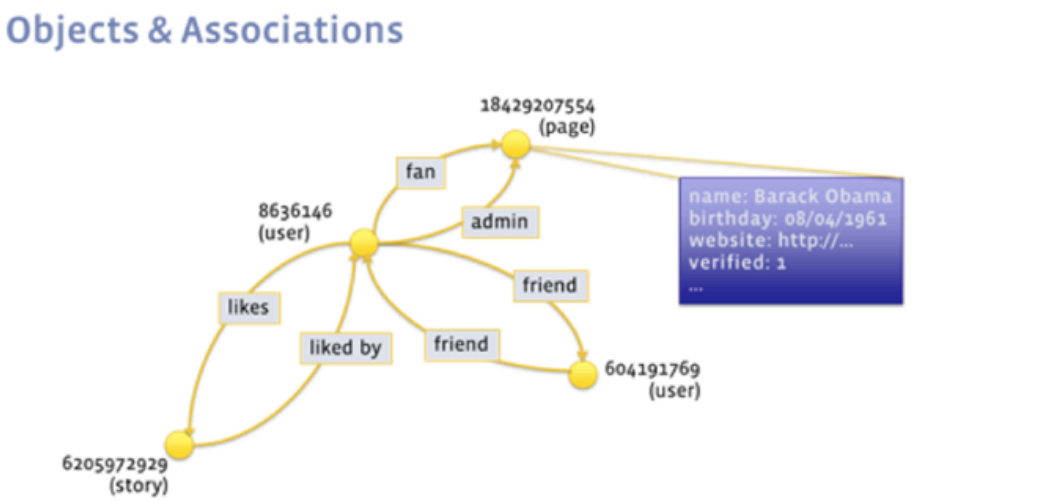

Figure 4. Facebook associations and objects [Marchukov, 2013]

Aggregation may take users' content out of context. In Figure 4, if a user 8636146 is a fan of a page "Barack Obama" then it can be suggested that Barack Obamas' fans like story 6205972323, which may not be true for all users who like Barack Obama page.

Data model illustrated in Figure 4 allows applications such as Tinder[14] to utilize existing user information and links with participants based on their likes and hobbies. This exposes users' data to more vulnerabilities on applications hosted by the third party services. Social networking services are designed to accumulate an immense amount of data. NoSQL databases such as TAO are effective in dealing with a large amount of data

[14] https://www.gotinder.com/ : A social networking application

for predictive analysis and historical data categorization [Kabir *et al*, 2009]. The issue however, is how data is used. Since data is immense, information can have various levels of access and various agents may use the information for different purposes. An example of which is illustrated in Figure 5.

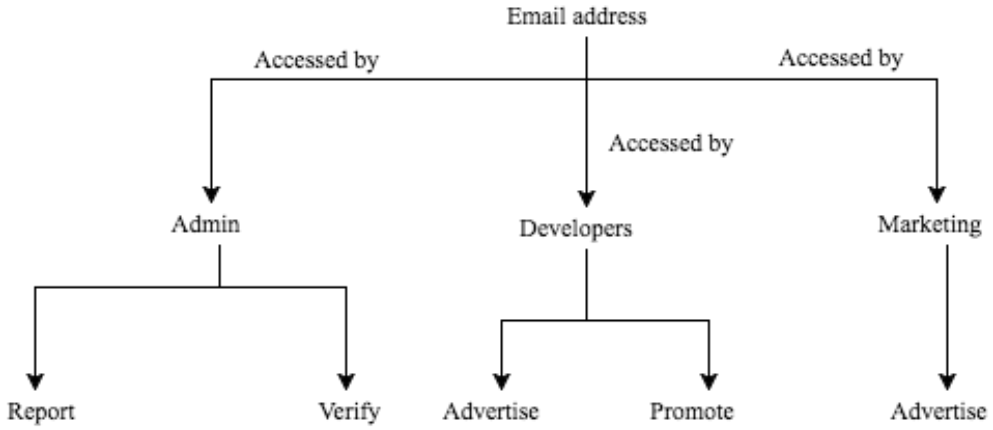

Figure 5. Data associations and purpose [Kabir *et al*, 2009]

For example, email address may be used by a system administrator to verify account or to report users a suspicious activity. In contrast, developers may use users' email address to advertise their application or to promote their content. Since users' data is accessible by third party applications, it may be used in a varying context.

It is not abnormal for SNS to store data for a long period of time. However, user must be in full control of any instance of data a user creates. Data retention may occur due to company policies and data duplication; some functionalities may also contradict with user privacy rights. As described in section 2.1.1, Facebook may store a list of friends that have been removed by the user. Whilst the information is hidden from the view of the user, it still exists in user database and hence this information is retained by Facebook, even though the user requested removal of information and all of its traces.

Cyber-stalking on SNS is inevitable. Users share their information within their networks, their content is shared on participants' wall and data outreach is magnified to the participants' wall as well. Social networking services should provide the means for a user to discourage such use. As stated in Facebooks privacy policy [API, 2015]:

> *"Technologies like cookies, pixel tags ("pixels"), device or other identifiers and local storage (collectively, "Cookies and similar technologies") are used to deliver, secure, and understand products, services, and ads, on and off the Facebook Services."*

Cookies are small files a website stores in users' browser; Facebook calls them "pixels". Pixels gather a users' activity from the third party applications that use Facebook for single sign on (SSO) or if the website or service is owned by Facebook.

Pixels are mostly used to gather insights on adverts. A user serving adverts via Facebook can tag a pixel along with the advert to receive insights.

Facebook can also communicate with users' device to gather new contacts to expand their network [O'Reilly, 2011]. There are several features on Facebook that cause concern over privacy. Since Facebook has a lot of data per user, it serves up to be a powerful search engine. A user can enter a phone number in search field and get a valid result. The problem arises when a person can iterate through series of numbers hence accumulating a list of people with their contact information.

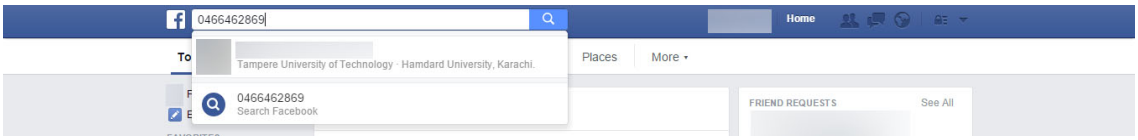

Figure 6. Facebook search

Apart from searching for phone numbers, users can also perform several other queries. Listed below are a few other attributes[15] a user may use to search for other users.

- People who work at x and like x
- People who work at x and live in x-city/state
- People who work at x who visited x-city/state
- Favorite interests of people who like x
- People who are not my friends that work at x
- People who are not my friends that live in x-city
- People who are not my friends that work at x and like x
- People who work with me at x

Some services may use location information to provide new and relative content, for example, location may be used to suggest nearby places to the user. Such services are called location based services. Location based services may share users' location episodically or constantly as they offer users to expand their network and socialize [Freudiger *et al*, 2011]. While location based services function as advertised, they pose a severe threat to users' privacy as they disclose personal information. Facebook also serves an API which allows developers to access functionalities from Facebook and user data. There are a few privacy concerns regarding implementation of API which will be discussed in following chapters.

Data collection, storage and destruction is another threat to user privacy. As highlighted by Facebook privacy policy 23 and 24 [Appendix A], Facebook is obliged to delete user data when their account is deleted, however, it is also phrased that data may

[15] http://wrightimc.com/2013/08/12/the-giant-list-of-facebook-graph-search-queries/

be kept until no longer needed. Problem associated with this functionality is that the user is no longer allowed to modify the data and correct it if there is any data distortion.

3.3 Privacy goal taxonomy

Security and privacy policies emphasize on integrity of personal data. Lichtenstein [1997] proposed a model to ensure development of internal security policies. The model proposes a four phase strategy which includes, requirements definition, design, integration and certification. Despite the existence of privacy and security policies, users "private" information is always at risk of being shared directly or indirectly. In 1999, fifteen graduate students collected information regarding private data from over 300 websites. The data was provided by Media matrix and the activity was funded by several companies. According to the results, 92.8% [Culnan, 1999] of the sample websites collected private data [1]; However, only 65.9% of the websites had posted a privacy disclosure documents for their users. The survey suggested that privacy policies documented by the services did not always comply with the practices adapted by the website provider [Antón *et al*, 2000].

Privacy goal taxonomy was proposed by Anton and Earp [2004] in which the GBRAM method is used to extract goals from documents such as privacy policies and then goals are classified into two categories which are Privacy vulnerabilities and privacy protection goals. Goals can be categorized as described in sections below. The authors subject each policy to scenario driven requirement elicitation process with a combination of goal analysis to extract security and privacy goals from policy documents.

3.4 Privacy protection classifications

Anton et al [2000] choose to use GBRAM method as it relies on no formal documents such as requirements documents or flow charts. GBRAM can make use of policy documents to elicit goals. Goals in requirements elicitation usually represent a state of achievement, whereas in this approach, goals may represent operational requirements of a system on a high abstraction level, furthermore, goals may be better at expressing functionalities and concepts to stakeholders as goals are represented in natural language.

Privacy protection goals represent the functionalities a system must satisfy. Privacy protection goals are reflected by the policies stated by the service on their website. These policies act as a guide for an end user and as a source of information on how their information is collected and stored. Privacy protection goals can be subdivided into five categories [Anton and Earp, 2004], which are: notice and awareness, choice and consent, access and participation, integrity and security and enforcement and redress (compensations).

For coming sections, scenario from Figure 3 can can be used to establish concepts of privacy protection and privacy vulnerability categories.

Privacy protection categories	Description	Example
Notice and awareness	A that user should and will be notified before data is collected and used within or outside the application.	Alice tags bob in her check-in. Bob is notified of check-in.
Choice and consent	A that a user must be given a choice of opting out of a said feature or data management practice. For instance, if user's data is to be used for say ads, user must be able to opt out of it.	Provided bob has enabled tag approval feature, facebook requires bobs' consent before he is tagged in the check-in.
Access and participation	A that user is always in command of his or her data. User may choose to edit the information anytime they want and have the right to restrict the usage of data anytime they want.	If bob disapproves the tag, bob is still allowed to view the check-in.
Integrity and security	A user must be aware of the practices involved in securing his/her personal information.	If bob is falsely tagged in the check-in, bob can report the tag to Facebook.
Enforcement/Redress	A user must be guided by the system or forced to follow a set of actions to preserve privacy.	If bobs' report on the check-in is valid, Alice's account may be disabled.

Table 3. Privacy protection goals

The definitions/categories explained above coincide with the privacy paradigms mentioned in chapter 3.1.1 (Privacy paradigms) and further stresses on the fact that privacy is a core concern of web based applications. For instance, Notice and awareness stresses that a user must be notified before any information is collected, used or shared whereas in privacy paradigms, transparency of information also promotes such behavior from the system as well as integrity and security and end to end security.

Similarly, enforcement/redress category stresses the necessity of having a system that promotes privacy by forcing user to chose secure settings which reflects the properties of privacy as a feature and not as a compromise from privacy paradigms. These categories will help to extract and analyze privacy policies and requirements of social media networks.

3.4.1 Notice and awareness

Notice and awareness principles suggest users' must be notified whenever information is collected from them or is transmitted elsewhere. The principle of notice and awareness

as suggested by [Anton and Earp, 2004], notice and awareness principles can be identified by following characteristics.

- General awareness and/or notice.
- Awareness when users' data is used by provider.
- Identification of parties that will receive the data.
- Clarification about what sort of information is collected.
- Steps taken by the collector to ensure confidentiality.

An example of notice and awareness can be taken from goals extracted using privacy policies of Facebook, which are highlighted in **Appendix A,** Requirement 2.17 (Notify users of suspicious login activity provides awareness to the user of an action that may include transfer of personally identifiable information (PII), where PII is any information that can lead back to the content creator. Similarly, goals elaborating what operations will be done on user data, as highlighted by Requirement 3.32, user data that is created publically will be shared publically.

3.4.2 Choice and consent

Choice and consent goals represents system behavior which allows a user to control what information is collected and what information is transmitted. Generally, in context of social networks these goals are represented by keywords such as OPT-IN or OPT-OUT. Choice and consent can also control functionality of how data is used by the provider, for instance, the user can choose not to index his/her data on search engine, or he/she can disallow specific users from viewing data. Having options though is not always favorable to the user, as the user could be overwhelmed with choices and may not always choose the best settings [Schwartz and Ward, 2004].

Policy 40, as listed in **Appendix A** represents functionalities associated with Facebook graph API. Graph API allows developers to use functionalities of Facebook, such as Facebook login to acquire user data from Facebook. However, Facebook provides choice and consent functionality to the user in almost every goal extracted from **Policy 40,** for example Requirement 9.6 [Appendix B] highlights the functionality where user consent must be acquired before developers' access user data.

3.4.3 Access and participation

Principle of access and participation emphasizes that a user should be able to access information at any time and should be allowed to modify it. Principle of privacy paradigm, transparency of information stresses how user should be able to control and view how the information is stored and used, that is, user must be able to selected the audience of their content. A perfect example of Access and participation can be taken

from Requirement 9.20 (Disallow developers access to object) where user can set privacy setting, which can change audience of user created content.

3.4.4 Integrity and security

Integrity and security principles implies that user data must be stored and processed securely. User should be made aware of the practices a provider may apply to secure user information from un-authorized access, misuse, data loss, and disclosure to un authorized users. Facebook mentions several policies emphasizing on functionalities that handle integrity and security. Requirement 9.5 (Disallow developers from accessing user information) suggests that user data is not disclosed to developers until they get proper rights from user.

Integrity and security principles may also suggest protection of user data through aggregation to hide PII, managerial and technical measure to protect user data from loss, application of user supplied data security settings and assurance of data control.

3.4.5 Enforcement and redress

Principles of enforcement and redress points towards steps an organization takes to assure user data integrity. Policies must suggest enforcement, otherwise they are merely statements [Antón *et al*, 2001]. Most of the providers fail to provide enforcement and thus a user has to rely on privacy documents and they must perceive whether and organization is adhering to supplied policies and data protection act (DP) [Griffiths and Remenyi, 2008].

Requirement 8.8 (Disable accounts of identified violators) is an example of enforcement, where accounts of users who spam on the service are disabled, furthermore, user is restricted from creating another account for a specific amount of time. Whereas Requirement 8.13 (Discourage users from collecting data) is merely suggestive as there are no implications if a user does not respect user privacy, hence Requirement 8.8 is an enforcement principle whereas Requirement 8.13 is merely an advice.

3.5 Privacy vulnerability classifications

While privacy goals ensure users of what they can expect in terms of security, whereas privacy vulnerabilities are the ways in which a user may face privacy violation. When user signs up to a service, they expect data integrity and control over the data, however, they might be unaware of a few privacy invasion phenomena's such as surveillance, monitoring, storage, transfer of information, information personalization and aggregation [Anton and Earp, 2004].

Privacy vulnerability categories	Description	Example

Information monitoring	The information is tracked by the service through cookies or any other services. The information might be used for statistical analysis, third party usage or perhaps surveillance.	Alice's check-ins are monitored to provide events and places closer to the last check-in.
Information aggregation	Personal information may be used along with data from other sources.	Previous check-ins of Alice may be aggregated with new check-ins to predict movement patterns.
Information storage	The data is stored within an organization.	Alice's check-in is stored under Alice's profile data.
information transfer	Personal information of a user is sold, distributed or made visible to a third party website.	Alice's check-in data may be transferred to authorities if requested.
Information collection	Information is requested by the organization or is provided by the user to the organization.	Location, time and date of Alice's check-in are collected.
Information personalization	Personalization of information on site, for advertising, offers or promotions	Facebook begins to offer
Contact	Scenarios where organization contact user for personal information.	Facebook offers campaign offers based on Alice's check-in.

Table 4. Privacy vulnerabilities

3.5.1 Information monitoring

Information monitoring goals reflect to an organization or a systems behaviour that monitors user data. Monitoring maybe beneficial in terms of security, however, these practices may also be used for selling aggregated information to the third parties [Anton and Earp, 2004]. Similarly, tracking usage behaviour may also indicate information monitoring, for instance, a user browsing internet for a new laptop being shown ads of cheapest laptops in and around users' location may point towards statistical collection for monetary purposes.

Requirement 2.4 (Monitor login activity of user account) implies that Facebook collects location, data and time of when user creates an account. This may provide functionality to service and can also be used to provide security features on the service. However, the goal is still categorised under privacy vulnerabilities. Some information monitoring goals may also highlight functionalities related to indirect data collection. Such is a case with Facebook where contacts from user device may be synchronized to suggest user new friends and invite more users to Facebook (Requirement 2.15). Whilst information monitoring can provide security features, the main concern is how and if the information is aggregated, would the user be notified? Would the information be taken

out of context? And can the information be used against the user? The use of monitored information is debateable [Mishra *et al*, 1998].

3.5.2 Information aggregation

Aggregation refers to combining old user information with newly provide information. Information aggregated may by PII in case of SNS. For instance, users' purchases may be aggregated according to spending limit and service may understand average user budget. SNS may also aggregate information for its features, for instance, Facebook aggregates old user pictures with new pictures to gather statistical data for automatic tagging, which itself (tagging) is prone to privacy vulnerabilities. Goals suggesting such behaviour are listed below.

Requirement 5.3 (Aggregate available pictures to suggest tags) implies that Facebook may use user pictures and perform facial recognition algorithms. While this would provide new features, users don't necessarily provide pictures in context of facial recognition and when they are aggregated, users' information may be taken out of context. However, not all goals directly highlight aggregation, for instance Requirement 6.10 (Receive browsing patterns from third party websites) does not explicitly suggest information aggregation, however, the gathered information is aggregated with existing information to suggest users; relevant pages and identical content.

3.5.3 Information storage

Information storage addresses how and for what reasons an organization stores user information. Information may be stored to perform activities around service for instance "collect user statuses" or for corporate activities such as "store users' transactions" [Anton and Earp, 2004]. On Facebook, nearly all of the information a user provides is stored [Policy, 2015], most of the information however, is used to provide features and ease of access to the user, for instance, Facebook stores user statuses and display them in a timeline.

While storing statuses and displaying them does not breach trust between provider and user, some data may be stored for organizational benefits. As illustrated by Requirement 1.4 (Store user information when user signs up for an account), Facebook collects information while a user signs up, information such as email address, name and phone number, while the attributes are necessary to run the service, the organization may also use this information to contact user regarding new marketing activities as highlighted by requirements 6.12 and 7.1. Services like Facebook rely on cloud services because of its' scalability, availability and elasticity. Cloud storage however can be associated with number of vulnerabilities such as availability, data protection, data control and duplicity [Jansen and Grance, 2011].

3.5.4 Information transfer

Information transfer refers to functionalities that allow user private information to be disclosed with other users or be indexed by other web services [O'Reilly, 2011]. Privacy by design does not allow information transfer, however, it is the core functionality of most social networking services since it allows a user to expand his/her network. Information transfer can mostly be identified using keywords such as *disclose, provide, sell, view* and *share.* Information transfer can lead to information duplication, identity theft or other privacy vulnerabilities.

As stated in Requirement 5.8 (Transfer user data partners, vendors, and providers), Facebook notifies its users that data may be transferred to family of companies which include a popular instant messaging service WhatsApp[16] and a photo sharing service Instagram[17]. This information transfer seems abundantly unnecessary as without this feature or action, Facebook can continue to provide service to its users. For this reason, information transfer is considered to be a privacy vulnerability.

3.5.5 Information collection

Information collection in social networking service occur in two different forms, direct collection of data where social networking services provides form to fill for instance when filling out a survey or filling out credit card information, or indirect collection where browsing data and other information regarding user activity is collected [Anton and Earp, 2004]. Facebooks' graph API also allows developers to collect information from users of Facebook, which broadens the scope of information collection. Listed below are the goals which exhibit collection behaviour.

Requirement 3.18 (Collect user conversation sent or received) illustrate how and what information can be collected by the service. Information collected can be used to provide features to the user and can be sold to advertisers and partner companies. Information collection can also prove beneficial where a user is asked for a feedback on a feature and provider decides on the basis of received feedback if the feature is early wanted. Thus, it becomes important that analyst carefully categorizes privacy vulnerabilities.

3.5.6 Information personalization

Information personalization refers to tailoring of user data to provide new features or customized for a specific user. Once user content is created, it is expected that data will be used in the context it was created in, personalization principles contradict with user expectations. An example of which can be taken from Requirement 7.1, where user data

[16] https://www.whatsapp.com: An application for instant messaging, owned by Facebook Inc.

[17] https://www.instagram.com/?hl=en: A social media application for sharing pictures

may be used to perform search operations on the service, where user may provide phone number for security purposes and it may be used by Facebook allowing users to search other users by their phone numbers.

3.5.7 Contact

The last element of privacy vulnerability as suggested by [Anton and Earp, 2004] is contact. Contact refers to goals in which a service or on organization may contact user. Sometimes contact can improve security of the system, for instance contacting a user for authorization or verification, but contact may by annoying when some other service contacts user on the basis of data collected from other service. Fortunately, there weren't many instances of contact goals extracted from privacy policies of Facebook, and which were extracted, suggested privacy protection more than privacy vulnerability.

3.6 Summary

As systems begin to evolve and start to collect more and more personal data, services like Amazon, Facebook and Google applications have begun to be more pervasive. Users rely on these services to carry out routine tasks such as socializing, shopping and even keeping track of daily schedules. More data we share on these services; more vulnerable we get with respect to privacy. Efforts are being made constantly to ensure user privacy and there are guidelines to ensure user privacy is always an issue of concern.

Privacy paradigms suggest a how privacy should be handled, however, due to large amount of data and countless number of cloud based applications used by a single user, privacy will eventually be compromised. This fact led Facebooks founder states that[18]: "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people," he said. "That social norm is just something that has evolved over time". If that is true, privacy invasion would not be considered inappropriate thus allowing SNS providers access to more personal information.

Whilst norm of privacy may have evolved with advancement of technology, it is still important to analyze impact of privacy vulnerabilities on user privacy. In order to establish vulnerability impact, requirements will be extracted from privacy policies of Facebook using Goal based requirement analysis method and privacy requirements will be extracted using taxonomy discussed in this chapter.

[18] http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov

4. Goal based requirement analysis method

Success of a software is determined by the degree of requirements and purpose it meets [Lapouchnian, 2005]. Inadequate, incomplete, inconsistent and ambiguous requirements had always been considered the key causes of incomplete and unsuccessful projects [Lapouchnian, 2005]. Goals were introduced to set a criterion for completeness of such software requirements where stakeholders are described as entities who strive to achieve a certain goal [Lapouchnian, 2005]. Whereas Anton and Earp [2004] describes goals as high level objectives as they describe the reason of why the particular system is needed.

User requirements are often documented as use cases [Wiegers and Karl 2013]. Use cases highlight courses of how a user interacts with the system to achieve a goals. The goal based requirement analysis method (GBRAM) is reverse engineering for a use case. GBRAM focuses on analyzing requirements based on goals. The GBRAM differs from other methods such as KAOS, *i**/troops, and non-function requirements (NFR) [Kavakli and Loucopoulos, 2003] framework in a way that GBRAM can use any available documentation such as policies mission statements etc. whereas other methods may require formal documentation [Lapouchnian, 2005]. Goals are determined in the process and are not mentioned anywhere else which makes it suitable for analyzing privacy requirements of social networking services [Lapouchnian, 2005].

While SNS promise safe and sound data storing and data management, there is no solid evidence if the policies are implemented internally [Karjoth *et al*, 2002]. A privacy policy is a comprehensive description of a website's information management practices. Privacy policies in contrast to requirements are broader in scope and may or may not be governed by regional or local legislations [Anton and Earp, 2004]. Privacy policies reflect the social norms and the values that are promoted in the community, whereas requirements may only reflect the organizations operational goals.

The language used in the process of requirements engineering can sometimes be too technical and may cause confusion and may result in unrealistic system requirements [Anton and Earp, 2004]. The Goal based requirements analysis model (GBRAM) is a straightforward method which identifies the enterprise goals and requirements [Anton and Earp, 2004]. The method refines the requirements on the basis of five principles, namely: identification, classification, elaboration, refinement, elaboration and conflict identification.

Anton and Earp [2004] Stated how the method of refining policies into natural language using GBRAM had turned out to be effective in e-commerce websites in their paper on *"A requirements taxonomy for reducing web site privacy vulnerabilities"*. E-commerce websites collect user's personal information and the authors deemed it necessary to analyze the e-commerce websites. However, more data is now being shared on social media websites than on e-commerce websites. Thus, privacy policies of social networking services must be analyzed.

4.1 Goal based requirement analysis model: Elements

The goal based requirements analysis model stresses that requirements should be treated as goals. Goals are more rational and hence easier to comprehend. The research paper by Anton and Earp [2004] made use of the GBRAM process to analyze privacy policies of e-commerce websites, a few key subjects are discussed in the research, which are listed below.

- Achievement goals: are the objectives the organization or system achieves. For instance, taking example of picture sharing on Facebook where a user's goal would be to share a picture with his/her friends only. The requirements for that goal would be divided into further sub categories, share photo, Select audience, Tag friends, **Limit** visibility. These four requirements may compose one goal of "sharing photos". Achievement goals are usually self contained and are refined into function requirements of a system [Anton, 1996].
- Maintenance goals: represent non functional requirements and define the scope of achievement goals [Anton, 1996]. Maintenance goals remain true unless and until a condition remains true.

Agents are initiators of an action and are responsible for achievement of a certain goal. An agent can be an automated process or a human. A human agent can be a moderator or and end user that performs certain actions, for instance an admin being responsible for integrity of the system.

Constraints of a system must also be identified; constraints are the conditions that must remain true to achieve a certain goal. Goal decomposition is another process which helps to uncover hidden goals, for instance a requirement highlighting publishing statuses can be broken down into, requirements such as: write a status, edit a status and share a status. Where agent in above decomposed goals is an end user.

Scenarios helps to identify and explore goals with perspective of other stakeholders and agents, publishing a status with respect to system can have a requirement: store status. Another process that can help to identify hidden requirements is analyzing goal obstacles. An obstacle may be identified while arranging achievement goals according to their precedence and also by negating the requirement statement. For instance, a requirement (status shared) may have an obstacle (status not shared). Analyst must then construct scenarios where a user may not be able to share a status.

The above mentioned elements helps to identify, classify, refine and elaborate goals. For instance, agents, stakeholders and constraints are key elements for identification process whereas scenarios and obstacles help to elaborate goals.

4.2 GBRAM process

In GBRAM, heuristics are rules and guidelines for analysts which help them to identify goals, requirements and other specifications of the system. Heuristics may be selected based on the information available to the analysts and availability of documentation. There are four types of general guidelines [Anton, 1996] that can be applied, which are listed in the Table 5.

Phases	Definition
Identification	Helps analysts to identify goals and requirements.
Classification	Helps determine type of each goal.
Refinement	Helps refine the sets of goals through some questions.
Elaboration	Addresses the need to acquire more detailed information.

Table 5. GBRAM heuristic classifications

The GBRAM is strategically categorized and the process initiates from exploring available documents. For GBRAM it is not essential to have a list of functional requirements and analysts can rely on documents such as workflows, policies, terms and statements, corporate goals and transcripts [Anton and Earp, 2004].

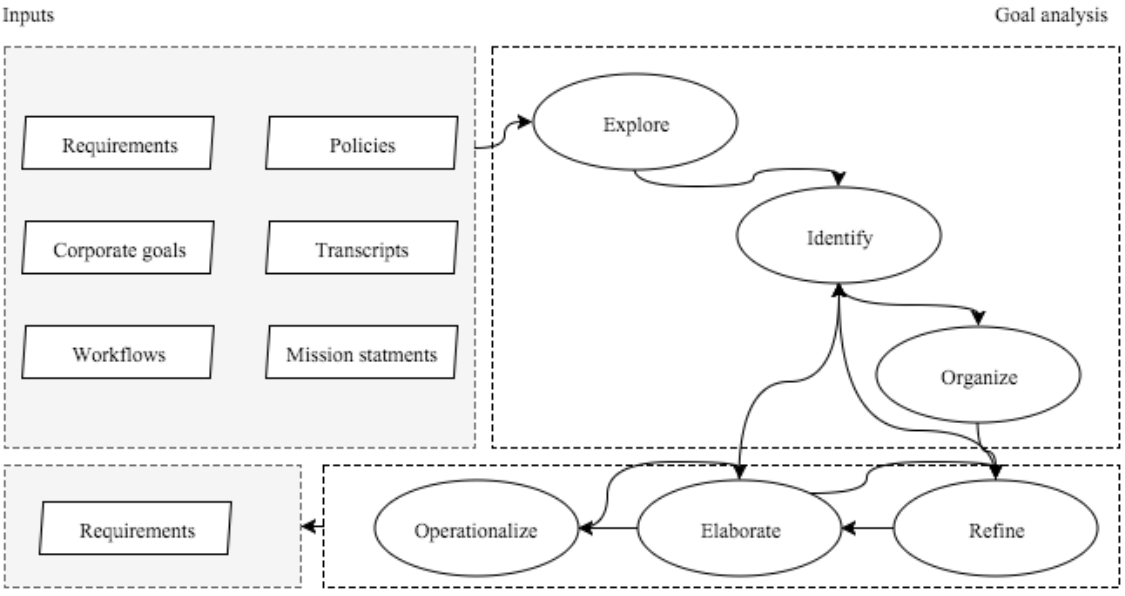

Figure 7. GBRAM process [Anton, 1996]

The process of requirement analysis starts from exploration. Exploration entails analysis of statements extracted from policies, requirements or other documents. Identification section of analysis extracts the requirements and agents associated with individual requirement and finally, organization of a requirement subjects it to a classification based on requirement dependency relation.

Process of refinement is used to prune the available requirements which allows the analyst to eliminate redundancies, eliminate duplicates and extract new requirements. Redundancies and duplications are removed by considering if a requirement means the same thing as another but worded differently to suit the agent. However, in such a case, all but one goal is eliminated. Redundancies are usually eliminated once the requirements have been ordered according to their precedence relation [Anton, 1996].

The process of elaboration pushes the analyst to discover hidden requirements by putting each requirement through a scenario. In the final step, operationalization helps to convert statements into readable requirements.

Objective of elaboration is to list out as much requirements as possible and to uncover hidden requirements that may not be listed in the documents. In order to do that, the analyst must study the environment closely. Operationalized requirements usually consist of achievement requirements as they map to actions that occur in the system and help analysts in specifying functional requirements [Anton, 1996].

4.2.1 Goal identification

The process of identification requires analysts to identify and analyze action words from fragments and identify stakeholders and agents [Anton and Earp, 2004]. The objective is to simplify the policies or documentation into simple words. The simplification of policy documents or requirement documents would help analysts define whether the requirement exemplifies the statement or is an obstacle for another requirement. The idea behind Goal identification would be to separate and identify verb actions, taking an example of one of the privacy policy listed by Facebook (Appendix A), policy 1.

> *"*We collect the content and other information you provide when you use our Services, including when you sign up for an account, create or share, and message or communicate with others. This can include information in or about the content you provide, such as the location of a photo or the date a file was created. We also collect information about how you use our Services, such as the types of content you view or engage with or the frequency and duration of your activities."

To identify requirements, an analyst must ask following questions.

- What requirements does this statement illustrate?
- What requirements would this statement obstruct?
- Does the requirement represent a state of avoidance?

Analyst must review the policy and use action words to extract requirements from the statement. The policy stated above can extract following requirements: account signup, create content, messaging service provided, share information, collect

information, store information, monitor location, share photos, monitor usage, and monitor frequency of usage. Requirements exhibiting avoidance may also be considered to extract fragments; avoidance represent a state that must be avoided in the system as highlighted by Requirement 8.13 which discourages collection of data.

A stakeholder is a person who is directly affected if a requirement is achieved or not. A stakeholder can be a user of the system, a third party service, an organization, or in case of Facebook, a developer as well. A goal must have one or more than one stakeholder associated with it where a stakeholder can be an agent, and an agent can be a stakeholder [Anton, 1996]. To identify stakeholders, the analyst could ask following questions.

- Who is directly affected by state of this requirement?
- Who and what claims a stake in this requirement?

Taking an example from requirements extracted from policy stated by Facebook, "Account signup provided", users, organization and system are direct stakeholders of the requirement. Signing up to an account would provide features of Facebook to the users, user signup would increase the number of registered users in the system and finally service provider would have one more user. Stakeholders are identified in the process of identification.

Agents are responsible for maintaining a state of the requirement or taking a requirement to a state of completion. An agent in case of Facebook can be a developer, a user, organization or for automated processes the system itself. Third party services may also initiate the process, however, system or organization may approve or disapprove third party from accessing information. For goal "Account signup provided", the system provides a signup form but a user is the one who is responsible for creating an account, hence, ultimately, user is the agent associated with the goal. The overall process of identification of goals, stakeholders and agents is highlighted by Anton [1996] in her dissertation.

4.2.2 Goal organization

A goal can be classified as either an achievement goal or a maintenance goal. An achievement goal is satisfied when a condition associated with the goal is achieved. Maintenance goals however, are those which remain true until their associated condition that is pre-condition or constraint remains true [Anton and Earp, 2004]. Hence, maintenance goals are usually mapped to non-functional requirements. Maintenance goals are usually extracted by asking following questions.

- Does the requirement ensure a state where some condition is held true throughout the process?
- Does the requirement suggest continuous state of achievement?

- Does the requirement affect decisions at various levels within the organization?

A set of keywords can be used to identify maintenance goals, the keywords may include verbs like maintain, keep, monitor, track, avoid, ensure, provide, supply, and know.

For requirements extracted from policy 14 from Facebook "share user content publically" suggests that users' content continues to be shared publically unless and until user changes the content accessibility. Agent involved in this requirement is the system, whereas stakeholders include both the system and a user; due to nature of continuation, the requirement is classified as a maintenance requirement. The classification is rather simple, as keywords provide an easy way to determine the classification.

Achievement represent requirement which are self-contained, a requirement which may depend upon completion of another requirement, a requirement representing a state of achievement or a requirement which would ultimately reach a state of conclusion.

- Does achievement of this requirement depend upon another requirement?
- Is ability of another requirement to complete dependant on current requirement?
- Does the requirement donate a state which has been achieved or a desired state?
- Is completion of this requirement self contained?

Common keywords that can be used to categorize requirements under classification of achievement include verbs like achieve, make, satisfied, allocated, completed, improve, speedup, and increase. However, any verb that signifies a desired state may be used to identify achievement goals.

For requirements extracted from policy 37 "Delete status" suggests achievement as it indicates a state of completion or awaiting an action. As highlighted earlier, achievement goals are usually associated with a target condition for instance, to delete a status, a user must create a status. Such relations help to extract new requirements and dependencies. In GBRAM, requirements are subjected to be organized according to their precedence relation or precedence dependencies. An analyst can ask following questions to determine dependencies.

- What requirements are prerequisites of current requirement?
- What requirements must follow current requirement?

Pre-conditions are requirements which become prerequisites of current requirement, whereas post conditions are requirements that must follow current requirement to achieve final result. A hierarchy can be constructed from this classification. An example of dependency can be taken from "Complete information collection". For this requirement to be achieved, a user must successfully create an account or log into existing account, create or share content, and finally, system will collect the information.

- Achieve account creation
    - Create content
        - Collect created content

The precedence of requirements can be represented in a form of: G1 > G3 > G4 where G1 is state of account creation, G3 state of creating content and G4 represents process of collection of information. Another way to represent requirement dependency is using graphing utility. Goal based requirement analysis tool GBRAT equates a similar result which helps analysts create better goal relations for the eventual SRD document.

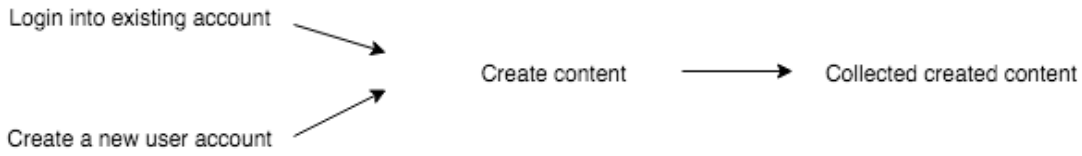

Figure 8. Hierarchal representation of goals [Anton, 1996]

Before concluding the phase of elaboration, an analyst must refine gathered requirements. Initially, requirements are refined if they are synonyms of each other, are duplicates of each other or if they are represented differently because of varying stakeholders in respective requirements. Refining requirements at stage of elaboration reduces work for the analyst and helps to reduce conflicts. Requirements extracted from Facebook policy document **"Monitor usage" "Monitor frequency of usage"** may be merged together since Monitoring frequency of usage would cover "Monitor usage" requirement.

So far, policy 1 [Appendix B] has yielded 25 requirements, classification of requirements resulted in categorization of 3 maintenance requirements and 25 achievement requirements, and dependency has elaborated a structure of operation.

4.2.3 Goal refinement

The process of refinement is carried out on each of the requirement extracted from process of identification after its classification and refinement done in section 4.2.2. The set of requirements will be pruned to further narrow down available requirements and then individual requirement will be elaborated which will construct scenarios in which a requirement can fail hence uncovering hidden requirements and dependencies. If a new requirement is uncovered, it is first classified, then refined and if it is still a valid requirement, it will be added to the list of requirements under a goal category.

It is possible to elaborate an individual requirement. For instance, "Account signup provided" may yield obstacles (a circumstance where a goal would fail) and constraints.

A simple way to identify obstacles is by negating a statement. In case of "Account signup provided" an obstacle can be identified as "Account signup not provided". The analyst must now think of a scenario in which a user can fail to create an account. Common keywords to find a scenario where a goal may fail include *however, not* and *when.*

In case of "Account signup not provided" an analyst can ask in which scenario account creation is blocked, an avid user of Facebook could answer this question quite easily as a user with an existing account is denied registration of another account and may log in with existing account. Hence, obstacle for G1 can be elaborated as "User already has a Facebook account" where as this scenario yields identification of two new goals, "Disallow multiple accounts" and "Login method provided".

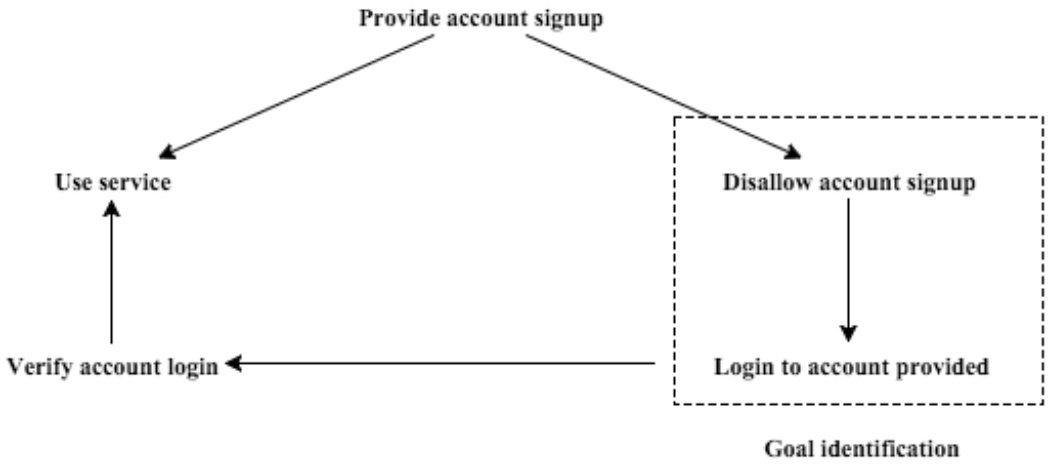

Figure 9. Goal elaboration process [Anton, 1996]

Identification of obstacles may result in either a precedence failure, a contract failure or an agent failure, where **precedence failure** occurs if a goal fails because the prerequisite goal failed to complete, agent failure due to irresponsibility of an agent, and when a contract relation fails then it is a **contract failure**.

To uncover scenarios, an analyst should ask why a goal failed? what are the actions available if a goal fails? did the goal have any contract binding goals? Did an agent cause goal failure? A single obstacle is usually associated with a single failure, for instance, failure to create content may fail due to its precedence that a user failed to authenticate to an account (precedence failure) or a user failed to authenticate into an account (Agent failure).

Goal	Goal obstacle	Scenario
Account signup	Disallow account signup	Account already exists (A)

Table 6. An example of scenario based elaboration

If a requirement cannot be refined or elaborated further, then it is subjected to constraint analysis. Constraints represent conditions that must be met for requirement completion. Generally, constraints can be identified by subjecting individual requirement to dependency analysis, where dependencies can be extracted using keywords such as before, during, after, and while. Requirement 2.8 highlights the Facebook may monitor user location, which can have a binding constraint with "Location monitoring enabled by the user".

The keyword "enabled" offers an indication that the feature may be disabled. If a user disables location monitoring service, then the requirement "Monitor location" would fail to achieve its final state and the resultant failure would be a **contract failure** because monitoring location requires location services to be turned on **while** user location is being monitored. In some instances, the service may ask the user the user to turn on location services, if user fails to do so then it will be an **agent failure,** whereas if application fails to verify if location services are turned on, then it will be precedence failure.

4.2.4 Goal operationalization

Operationalization is required to convert extracted goals into a formal form of specification. Each requirement is traced back to its original statement and then mapped onto actions to give a form of a schema. A schema may not be a very formal representation of defining requirements, however, it represents behavior of a requirement under certain circumstances which can be read by general audience having little to know knowledge of requirements engineering. A schema as defined by Bartlett and Burt [1933] is:

> "An active organization of past reactions, or of past experiences, which must always be supposed to be operating in any well-adapted organic response"

The definition suggests that schemas are organized and well adapted. A schema for GBRAM process as defined by Anton and Earp [2004] can have a following specification.

Requirement 1:	Name
Policy:	Number
Type:	Classification
Action:	After operationalization
Agent:	Name
Stakeholder:	Name(s)
Constraints:	Item(s)
Obstacles:	Item(s)
Pre-condition:	Condition(s)
Post-condition:	Condition(s)
Sub-goals:	Item(s)

Table 7. Schema defined for GBRAM

The elements in scheme described above has following elements:

- **Requirement: Name**
  A requirement is an objective a system must meet. Requirements may have associated constraints or be blocked by other requirements and may be divided into sub goals and then operationalized. Requirements should be worded to describe a desired state.

- **Classification: Name**
  A Requirement can be classified as either a maintenance goal where maintenance goals are true until a goal blocks them, or an achievement goal which occurs when a condition is true.

- **Action: Name**
  Name of the requirement after operationalization.

- **Agent: Name**
  Agent is responsible for achieving a requirement. An agent can be a user or an automated process.

- **Stakeholder: Name(s)**
  Stakeholders are those entities, which are effected by the state of the requirement. A requirement must have one or more than one stakeholder associated with it.

- **Constraints: Item(s)**
  A constraint describes a condition or an activity that must be met before a requirement can reach state of completion.

- **Obstacles: Item(s)**
  Obstacles are statements, which highlight the activities that may block the requirement from occurring. An obstacle can be a general failure, a prerequisite failure, an agent failure or a contract failure.

- **Pre-conditions: Condition(s)**
  Represents a condition that must be met before specific requirement can be completed. The requirements are ordered according to their precedence to highlight failure if previous requirement is left unmet.

- **Post-conditions: Condition(s)**
  Post-conditions depict a behavior that may follow upon completion of current requirement.

Functions are represented in a form of formal operation definition, each requirement must be associated with at least one operational definition, however there may be instances where one requirement has more than one operation definition, each for a user and system or other entities of system.

After the evaluation of selected policies and documents, the resultant goal set have a total of 136 requirements. However, it may be more appropriate to call these goals requirements. The requirements then can be broken down into objectives or goals. Since goal organization requires that achievement goals be sorted according to their precedence, it becomes convenient to identify objectives. Hence, identified goals on Facebook are as follows.

Account signup: requirements under account signup goal highlight the processes required to achieve account signup. The requirements are organized according to their dependency relation. The dependency relation is shown in Figure 10.

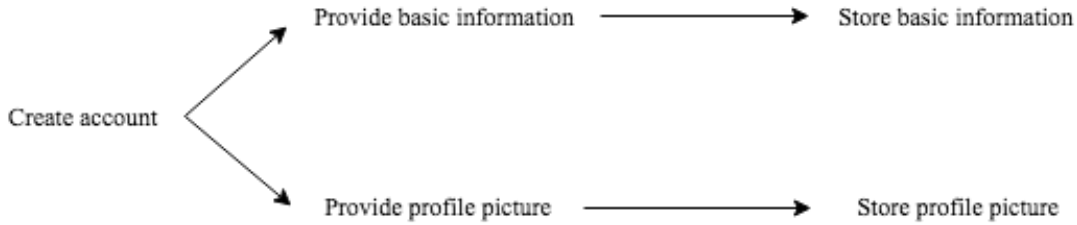

Figure 10. Account signup activities (Appendix B, goal 1)

It is important to note that since requirement 1 (Prevent multiple accounts from user) is classified as a maintenance requirement, it is ignored from the hierarchy as it is not dependent on any other activities under the goal classification (Account signup).

Account login: requirements classified under account login activities highlight the activities a system or a user performs to achieve login state. The hierarchy of account login activities is highlighted in Figure 11.

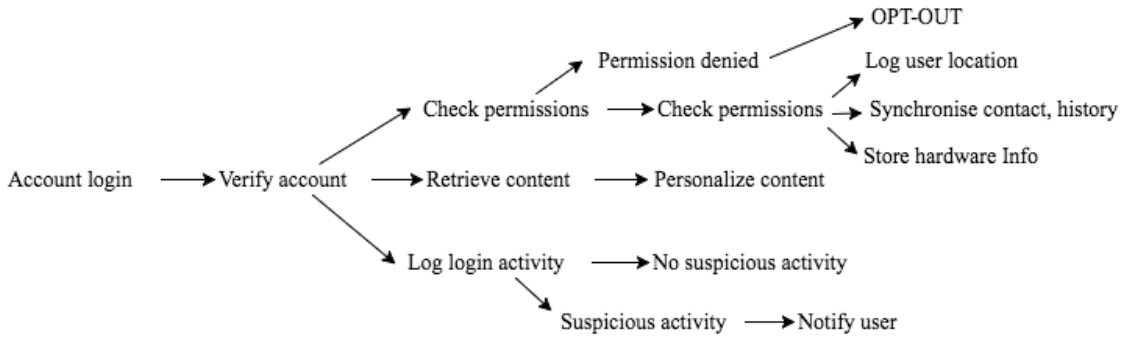

Figure 11. Account login activities (Appendix B, goal 2)

User activities: requirements highlighting functionalities or actions user may perform on Facebook. User performs an activity, the system collects and stores the information.

A User may sometimes be allowed to modify and delete the information as well. The hierarchy is illustrated in Figure 12. It is important to note that the figure represents abstract process of creating, storing, modifying, deleting and downloading content. The requirement create content includes creating statuses, images, videos, tags and other activities on Facebook.

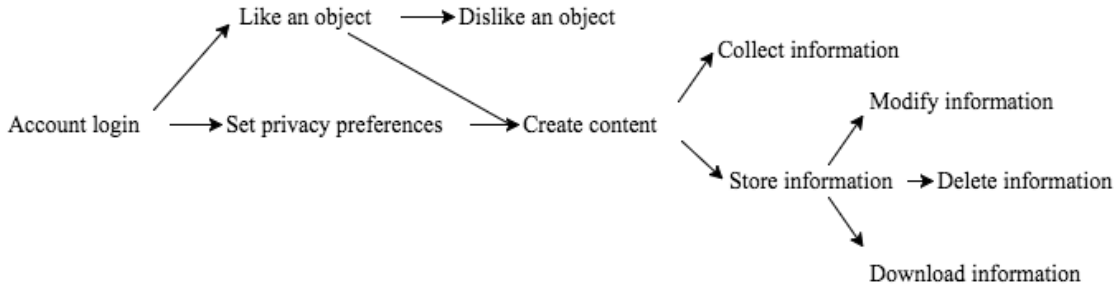

Figure 12. User activities (Appendix B, goal 3)

Purchasing activities: A user on Facebook may initiate payment activities by purchasing advertisement services, sending gifts over Facebook or paying for sponsored content. These activities have a hierarchy as shown in Figure 13.

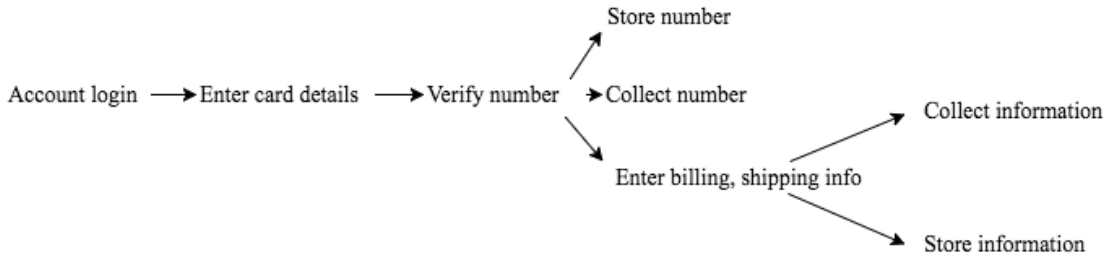

Figure 13. Purchasing activities (Appendix B, goal 4)

Behind content creation: Some activities may be hidden from user view, such activities usually suggest indirect data collection, such as monitoring location, storing information about friend etc. The hierarchy is illustrated in Figure 14.

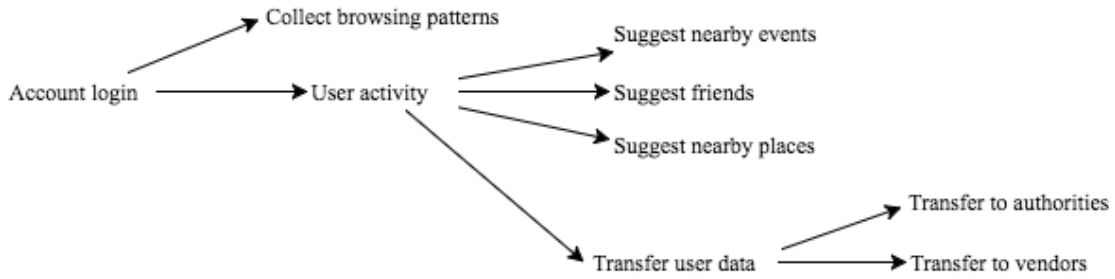

Figure 14. Behind content creation (Appendix B, goal 5)

Advertisement activities: User data may be used to provide relevant advertisements on user timeline. Users may also choose to purchase advertisement services to promote their content, page or a group. The processes are listed in Figure 15.

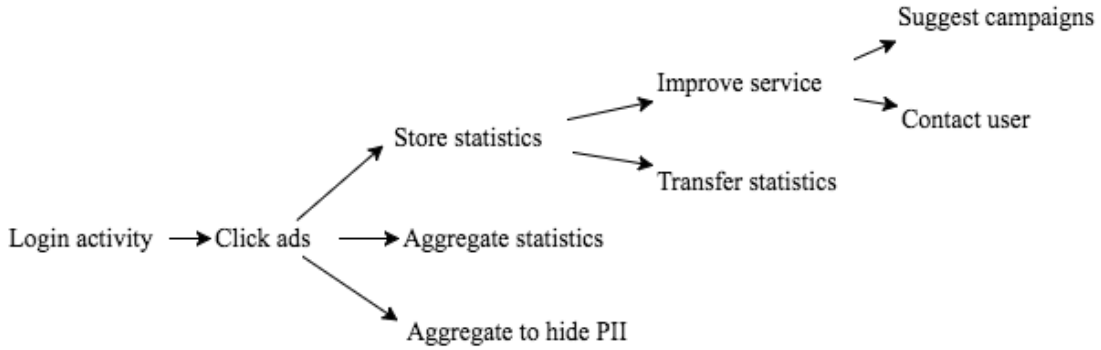

Figure 15. Advertisement activities (Appendix B, goal 6)

Data usage: Users' content stored on Facebooks' servers may be used over time for advertisements or to provide features on the service. Perhaps one of the most known feature is the graph search. Using graph search, a user can be searched with their phone number, email, address, location, gender and other related information. These however are maintenance goals. Achievement goals highlighting usage of data are illustrated in Figure 16.

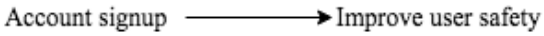

Figure 16. Data usage on Facebook (Appendix B, goal 7)

Integrity and security: Facebook handles a lot of personal information. It is essential that Facebook provides security features to establish trust between the user and system. Requirements highlighting integrity and security features are shown in Figure 17.

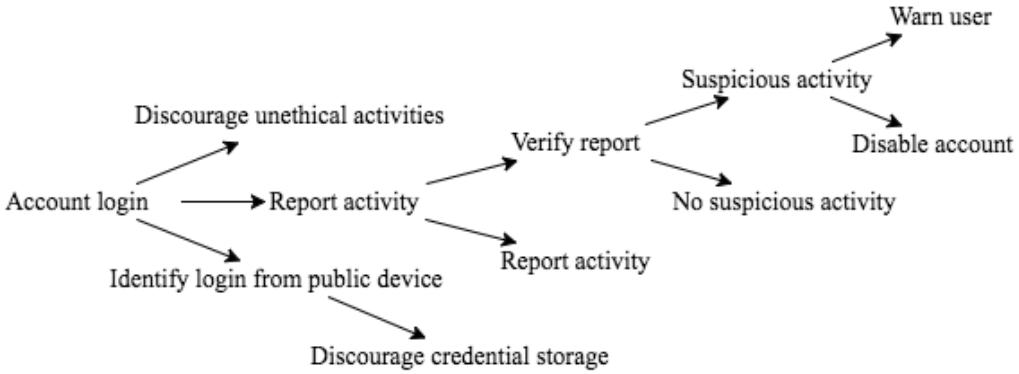

Figure 17. Integrity and security (Appendix B, goal 8)

Facebook API: Facebook provides an application program interface (API) through which developers can access user data for their applications. Developers can access

public user data or private data when they get required consent approved. The hierarchical structure is illustrated in Figure 18.

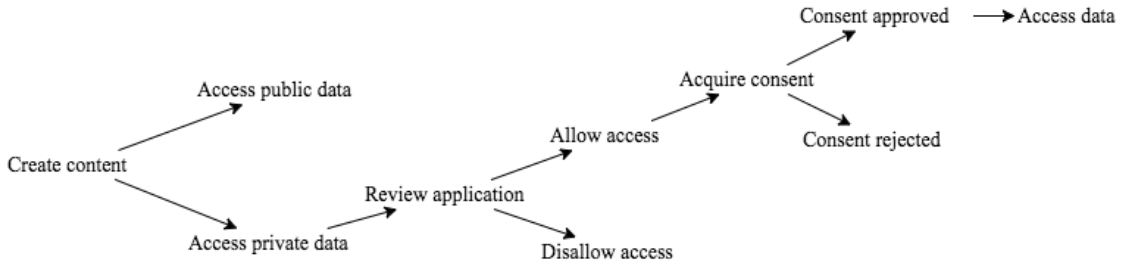

Figure 18. Facebook API (Appendix B, goal 9)

Data management: From account creation to deletion, user data is created, collected, aggregated stored and transferred. Facebook may make copies of user data to ensure availability, for this reason, deletion may not always ensure erasure of data. Data management practices are illustrated in Figure 19.

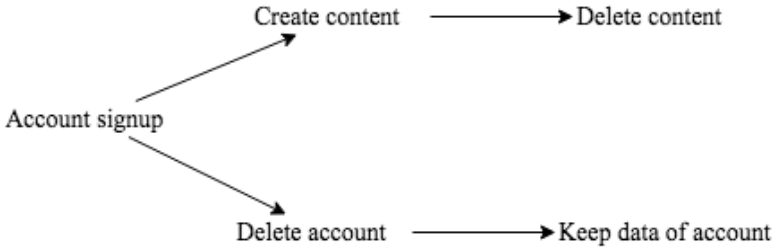

Figure 19. Data management (Appendix B, goal 10)

Once requirements have been sorted according to their precedence, privacy taxonomy can now be applied to the resultant set of requirements to get privacy related requirements.

4.3 Summary

The process of GBRAM is elaborated in chapter 4, which allows the analyst to review requirements of a system using available documents. The process of identification extracts goal sets and identifies stakeholders who are affected by the goal and agents who are responsible for completing a certain goal.

The second phase requires analyst to classify goals. Goals can be classified as either maintenance goals or achievement goals where achievement goals are usually self contained and may depend on other goals to begin processing, for that, several types of dependences have to be studied, which include precedence dependency, contract dependency and agent dependency. Maintenance goals continue to perform an action till the condition remains true and generally, they do not rely on other goals to be processed.

Organization of goals also requires that achievement goals be listed in a hierarchy, which according to their precedence relations, this helps analysts to uncover hidden processes and goals.

Goal refinement is a process where a goal set is reduced by eliminating redundancies and reconciling synonyms. While reconciling synonyms, the analyst must make sure that goals being reconciled are classified under the same category, as either an achievement goal or a maintenance goal. During refinement process, scenarios are also considered which further helps to understand hidden goals and features. In the following chapter, identified goal set would be studied under privacy taxonomy suggested by Anton which will help uncover privacy protection and privacy vulnerability goals.

5. Privacy vulnerability analysis

GBRAM defines a process which takes document(s) as an input and produces set of requirements as an output. In the case of Facebook, the privacy policy document, the cookie policy document, the terms and condition document, the Facebook graph API workflow, and Facebook data storage workflow are the inputs. The resultant goal set derived using the GBRAM process include a total of 136 requirements after elaboration and refinement, out of which, 42 requirements were classified as maintenance requirements and 92 as achievement requirements.

Set of goals are arranged according to their subject and their precedence. Each subject has a set of requirements. Ten identified goal categories are: Account signup, account login, user and system activities while using the service, purchasing activities performed by user on Facebook, background activities when user creates content, advertisement services on Facebook, usage of data, integrity and security, Facebook API, and data management practices. Once the goal set have been identified, privacy taxonomy proposed by Anton [2002] is applied to each requirement in the goal set to identify privacy protection requirements and privacy vulnerabilities.

The approach of goal classification has already been discussed in chapter 3, now that the requirements have been extracted from available documents, each requirement within a goal category can be categorized as either privacy protection or a privacy vulnerable requirement. Requirements suggesting privacy protection properties are listed in Table 8 along with their requirement number which corresponds to the goal category, policy that was used to extract the requirement and a brief description of the requirement.

Privacy protection	Req	Policy	Description
Notice and awareness	3.30	9	Notify users when they are tagged
	3.32	14	Share user content with public
	3.33	14	Share content with friends
	3.34	14	Share content with custom audience
	3.35	14	Share content with friends of friend
	3.41	28	Notify user of suspicious login activity
Choice and consent	2.11	10	OPT-OUT of location services
	3.27	9	Verify whether users can be tagged
	3.31	14	Privacy settings provided to the user
	9.6	39	Acquire user consent before sharing data
	9.18	40	Require consent with rights to object
Access and participation	3.4	37	Modify existing status
	3.5	37	Delete existing status
	3.9	37	Delete created photo, video
	3.13	37	User dislikes an object
	3.17	37	Delete started conversations
	3.28	9	User approves a tag
	3.29	9	User disapproves a tag
	8.4	13	Allow users to report suspicious activity

	9.19	40	Allow developers access to object
	9.20	40	Disallow developers access to object
	10.1	23	Allow users to delete their account
Integrity and security	1.1	1	Prevent multiple accounts from user
	2.2	1	Verify signup and login activities
	2.17	28	Log login activity to prevent unauthorized access
	6.8	12	Aggregate statistics to hide PII
	7.2	13	Encrypt user data
	8.3	32	Route traffic to improve service
	8.5	13	Verify reported activity
	8.16	38	Identify access from public computers
	9.3	39	Review application requiring private user data
	9.5	39	Disallow developers from accessing data
Enforcement and redress	8.8	13	Disable user account if violating privacy
	8.9	33	Prevent spammers from using the service
	8.11	34	Prevent policy violators from using the service
	8.12	38	Discourage users against posting spam
	8.13	38	Discourage users against collecting data
	8.14	38	Discourage users' against harassment
	8.15	38	Discourage users against violating privacy
	8.17	38	Discourage saving credentials on public computers.

Table 8. Privacy protection requirements

On contrary, privacy vulnerable requirements usually put the user data at risk to monitoring, personalization, aggregation, storage, collection, transfer, and for improper use; such as for marketing updates and un-wanted contact by the SNS. The privacy vulnerable requirements are illustrated in Table 9.

Privacy vulnerability	**Req**	**Policy**	**Description**
Information monitoring	2.4	28	Monitor login activity of active user account
	2.6	30	Monitor language and region of logged in account
	2.15	5	Synchronize contacts, browsing history from users' device
	5.1	1	Track browsing patterns
	8.1	29	Monitor users' transactions
	8.2	31	Monitor active friends of the user
	8.10	34	Monitor off service usage to track underage users
Information aggregation	5.3	9	Aggregate available pictures to suggest tags
	6.5	12	Aggregate available information to display relevant ads.
	6.10	7	Receive browsing patterns from third party services
Information storage	1.4	1	Store name, email, date of birth and gender of the user
	2.5	1	Store login time and date
	2.10	10	Store the user location at login
	2.14	5	Store hardware information and IP addresses from device used to access Facebook.
	3.3	23	Store created status

	3.8	23	Store created photo, video
	3.12	23	Store the user likes on an object
	3.16	23	Store the user conversations sent or received
	3.20	23	Store user created check-in
	3.24	23	Store information of friend user added
	3.39	1	Store time and date of content creation
	3.40	37	Ensure data availability by making copies of the data
	4.9	23	Store credit/debit card number
	4.11	23	Store shipping, billing information
	10.2	23	Keep data of deleted account
	3.41	37	Store name of deleted friend of user
Information transfer	5.7	25	Transfer all available information to authorities
	5.8	21	Transfer data to partners vendors and providers
	6.9	12	Transfer advertisement statistics to advertisers
	9.9	40	Share the user game activities with developers
	9.10	40	Share the user photos with developers
	9.11	40	Share the user comments with developers
	9.12	40	Share the user messages with developers
	9.13	40	Share the user events with developers
	9.14	40	Share the user friend list with developers
	9.15	40	Share the user content from groups with developers
	9.16	40	Share the user likes with developers
	9.17	40	Share the user photos with developers
Information collection	2.13	5	Collect hardware information and IP addresses from device used to access Facebook.
	3.2	1	Collect created statuses
	3.7	1	Collect created photos and videos
	3.11	1	Collect users' liked objects
	3.15	1	Collect the user conversations
	3.19	1	Collect check-ins created by the user
	3.23	1	Collect information of friend user added
	4.8	1	Collect credit/debit card number
	4.10	1	Collect billing, shipping address
	5.2	2	Collect information in which the user is tagged
	6.4	1	Collect browsing patterns of user off the service
Information personalization	2.7	30	Personalize profile with language and region
	5.4	10	Use location services to suggest nearby events
	5.5	10	Use location services to suggest nearby places
	5.6	10	Use synchronized contacts to suggest new friends
	7.1	9	Use available information to provide search features
Contact	6.12	11	Contact the user to offer new marketing campaigns

Table 9. Privacy vulnerable requirements

While categorization of requirements as either a vulnerability or a protection requirement provides an overview, the process does not study the impact of vulnerability on an end user. Furthermore, a requirement categorized as a vulnerability may not always prove to be a risk to a users' privacy as there may be obstacles, constraints, or pre-conditions preventing those requirements from being achieved. As highlighted in goals

extracted [Appendix B], goals have obstacles associated with them and it is worth considering if those obstacles can reduce the impact of vulnerability.

5.1 Vulnerability classification

A complex information and communication system may give rise to vulnerabilities related to design, implementation and management. These vulnerabilities in return may result in privacy invasions [Arbaugh *et al*, 2000]. Vulnerabilities however may differ in severity and may be unjustly classified as a vulnerability. For the requirements extracted from privacy policies of Facebook, the vulnerable requirements represent potential privacy flaws in the system, however, some vulnerabilities may not pose a threat to users' privacy. For example: Requirement 1.2 (Provide account signup option) is a necessary feature which is required to use the service, but, since Requirement 1.2 reflects system behavior of storing and collecting information, it is initially classified as a vulnerability.

Vulnerability classification method suggested in section 5.1.2 can help an analyst categorize vulnerabilities according to the risk they pose on users' privacy and even help to eliminate requirements from goal set which are are deemed invulnerable to the user privacy.

The most prominent subject matters' extracted from vulnerable requirements relate to user location monitoring, monitoring user activity, indirect data collection, direct data collection, information aggregation, advertisements, data transfer, network information collection, information sharing and credit card information. Location monitoring in an untrusted environment is a grieve threat to user privacy, as information can easily be abused, provided, a user cannot disable these services. An example of which can be taken from an infamous application called murderers map. This chrome[19] extension acquired user location through Facebook graph API and displayed on a map, there was noticeable backlash from Facebook users regarding the exploit and Facebook removed the feature from graph API [Khanna, 2015].

However, before vulnerabilities can be rated according to the threat they pose on users' privacy, its is important to understand what information is private to the user. Since some users' may consider location monitoring a privacy vulnerability and others may not, it is important to study users' perception on privacy.

5.1.1 Data collection and interviews

In order to study the user perception on privacy, questionnaires and interviews were prepared. Software developers who are active users of Facebook and with knowledge of Facebook API were chosen to participate in the interview and questionnaire. An active user has a better understanding of privacy settings and over all functionality of Facebook,

[19] Chrome is a popular internet browser developed and maintained by Google.

thus they were preferred over new users of Facebook. In total, 15 developers participated in the activity. As it has been stated earlier, the definition of private information varies from a user to another. Understanding what subject matter is private for an end user would contribute to privacy vulnerability analysis.

The interview phase of the questionnaire was conducted to determine the user awareness on privacy settings on Facebook and the consequences of turning these settings off. Another agenda of the interview was to discuss the data management practices used by Facebook. Participants were queried about data collection, storage, aggregation, and data usage activities performed by Facebook. Indirect data collection such as contact synchronization, location monitoring and collection of browsing patterns were also discussed in the interviews.

The questionnaire part has 26 questions which include multiple choice, and scaling questions; mainly emphasizing on the user awareness regarding potential privacy flaws on Facebook. The questions mainly quizzed the participants regarding privacy settings available to an end user on Facebook. The questions were mostly derived from the concepts of privacy paradigms. Privacy vulnerable requirements were also used to quiz participants to understand their perception on privacy. For example, question 9 of the questionnaire [Appendix C] asks the participants whether they consider background synchronization of contacts from users' mobile device a vulnerability. The question was derived from Requirement 2.15 (Synchronize contacts, browsing history from users' device) [Appendix B].

Short interviews were conducted to gain an insight on the ability of an active user to manipulate and understand privacy settings on Facebook. Question 5 [Appendix C] was asked from the participants, where, 12 participants were unable to change location monitoring preferences. Question 18 [Appendix C] which corresponds to question 5, was asked to understand the perception of the participants on the subject of location monitoring. A common suggestion was that if a users' location is to be monitored, pre-conditions, obstacles and constraints must be associated with such requirement, if not, then the user must always be notified if and when their location is monitored.

Question 19 [Appendix C] queried participants regarding the background data synchronization, such as synchronization of browsing history and contacts from user device. Participants highlighted that if there was a pre-condition, an obstacle or a constraint associated with such requirement and if those measure were not to be configured manually, then they would not be bothered by background data synchronization. However, the participants also emphasized that the SNS must ensure that such information is not transferred to other entities such as advertisers, partner companies, and authorities.

The participants emphasized that a user must not have to explicitly define a privacy setting for any feature that shares personal information. According to the questionnaire,

most of the participants suggested that their photos, location, contacts, phone number and credit/debit card numbers are private. A few other concepts such as value and crucial functionality were mentioned by the participants. Where, a requirement may suggest value to an end user, for example Requirement 3.10 (User likes and object) [Appendix B], and alternatively the requirement may suggest activities that provide value to the business as suggested by Requirement 6.4 (Aggregate available information to display relevant ads) [Appendix B].

Concept of crucial functionality on the other hand suggests that a requirement must not exist without a reason. If eliminating the requirement and the associated functionality does not effect end users' experience on the service, then the requirement is not crucial. Based on the interviews and the questionnaires, following focus points are established which helped to create privacy vulnerability reduction process as illustrated in Figure 20, Figure 21, and Figure 22.

- Requirements classified as vulnerabilities must have a pre-condition, a post-condition, a constraint or an obstacle preventing the vulnerable requirement from being achieved. Such conditions must be system initiated to exhibit 'privacy by default' rather than controlled by the user manually.
- If vulnerability prevention is not provided, then user consent must be acquired before the user data is used.
- A requirement may exhibit business value, such as aggregating usage statistics and providing data to advertisers. Requirements may also suggest value to an end user, such as monitoring login activity to notify users of about suspicious login activity. If user consent is not acquired, then the requirement must exhibit value for an en user.
- If no value is provided to an end user, impact of vulnerability on a user and his/her friends has to be considered. However, no privacy vulnerability prevention as a default measure or choice and consent means that the vulnerable requirement may not be eliminated from the list of vulnerabilities. However, if privacy settings can be adjusted by an end user to prevent achievement of a requirement, then it is less vulnerable to users' privacy, otherwise it is vulnerable.
- Lastly, if no value is provided and personal information of user is used without consent, notification must be provided to the end user. If there is no notification provided, then the requirement is considered highly vulnerable to users' privacy.

Using information collected from the questionnaires and the interviews, risk evaluation categories are constructed and are listed in Table 10.

Vulnerability	PII	Choice	Crucial functionality	Value	Privacy feature
Low	No	No	Maybe	Yes	Yes

Vulnerable	Maybe	No	Maybe	Yes	No
High	Yes	No	No	No	No

Table 10. Vulnerability classification

5.1.2 Vulnerability assessment process models

Considering the results derived from the interviews and questionnaires, inclusion of some requirements as vulnerability seem unjustified. For this reason, vulnerable requirements exhibiting privacy vulnerability prevention via constrains, obstacles or pre-conditions should not be considered vulnerable. However, the system is also responsible for providing settings appreciated by the user, hence, privacy protection should be enabled by default. If a user still has to manually provide settings to secure that information, the feature remains vulnerable, provided, consent is not acquired from user and service can continue to perform if the feature is eliminated

Privacy paradigms (3.1.1), results from the interview and analysis of goals extracted using GBRAM contributed significantly in defining a method to analyze privacy vulnerable requirements. The key elements that contribute to the method include concepts like proactive than reactive, a default measure, privacy as a feature and not as a compensation, and respect for user data and privacy. The privacy vulnerability analysis can be broken down into three steps: Privacy by default, choice and consent, and notice and awareness.

When vulnerabilities have been identified a few questions can be asked to evaluate impact of a vulnerability on users' privacy. The first step is derived from privacy paradigm (section 3.1), privacy as a feature and not as a compensation and response from interviews conducted specifically question 23 [Appendix C] which asks about the user insecurities regarding data management practices. The interviewees highlighted that if a pre-condition suggests privacy protection of the requirement from being vulnerable, the it may not be considered a vulnerable one. However, it was also highlighted that such features must be activated by default.

In hindsight, the principles justify findings from the interview. Privacy paradigm principle "a default measure" suggests privacy must set by default and privacy as a feature suggests privacy features must be associated with requirements. The participants from the interview also signified the importance of having privacy requirement for every feature. Similarly, respect for user data and privacy signifies the importance of usage of personal user information and how information must only be used when absolutely necessary, as suggested by the interviewees as well.

The first phase of requirements vulnerability analysis is to find out the whether the identified requirements meet the criteria of privacy by design. The process us illustrated in Figure 20. Privacy by design.

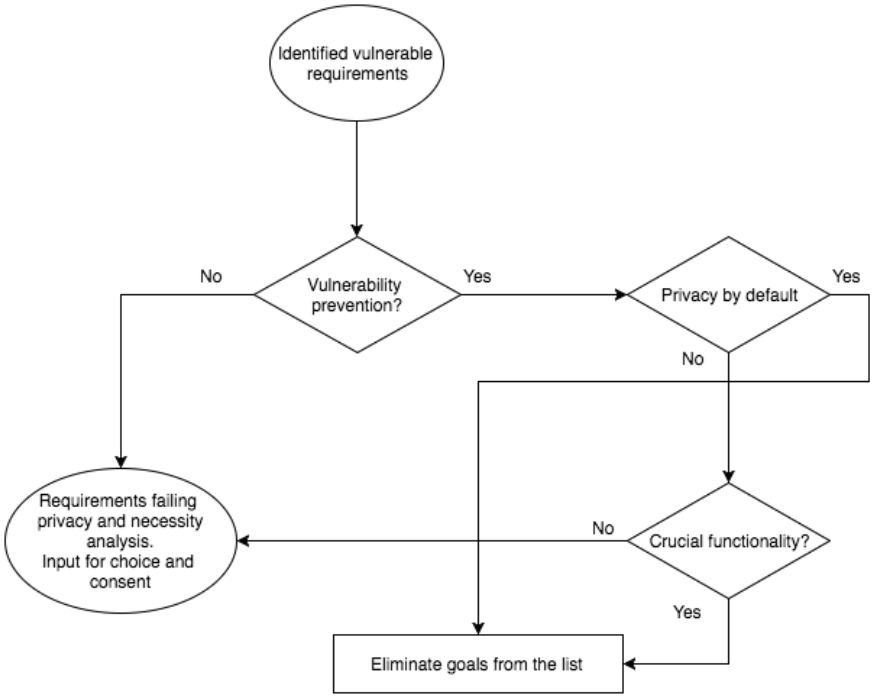

Figure 20. Privacy by design

From initial inspection, monitoring activities usually suggest vulnerabilities. But upon considering the facts gathered from literature review, interviews, and questionnaires, it was determined that eventually Requirement 2.4 provides security features to the user and hence it is eliminated.

If a requirement does not meet the criteria of of privacy by design, choice and consent classification must be applied to determine vulnerability severity or to eliminate requirement from vulnerability classification. Privacy paradigms (section 3.1), suggests that user data and privacy must be respected, whereas Anton and Earp [2004] highlight choice and consent as one of key elements of privacy protection classification.

Choice and consent gives the user the power to control whether their information is used or not, however, transparency from service provider regarding data management practices are essential if requirements exhibiting choice and consent are to be eliminated from vulnerability classification.

For the interest of the user, if PII is used, then the feature must provide crucial functionality. If it does not use PII, it may be eliminated from vulnerability classification. If no choice and consent, the requirement must exhibit some value to the user, if not then it may be classified as a highly vulnerable, vulnerable or low vulnerable one. The process is highlighted by Figure 21. Choice and consent.

Figure 21. Choice and consent

Some features may affect the privacy of a users' friend. Considering Requirement 3.26 (Tag friends on network) [Appendix B], whenever a user tags another user in a picture on Facebook, the target picture becomes part of friends' data as well. This broadens the scope of visibility of the content and increases the chances of duplication, and misuse. Therefore, such a requirement may not be eliminated from the list of vulnerable requirements. The requirement may only be classified as either a low vulnerable one or a vulnerable requirement, where the requirements may not be considered highly vulnerable as long as they don't share, transfer personally identifiable user information, where vulnerability classification is highlighted in Table 10.

The third step in the process only classifies the requirements as being vulnerable or highly vulnerable as they use users' personal information without user consent and without providing value to the user.

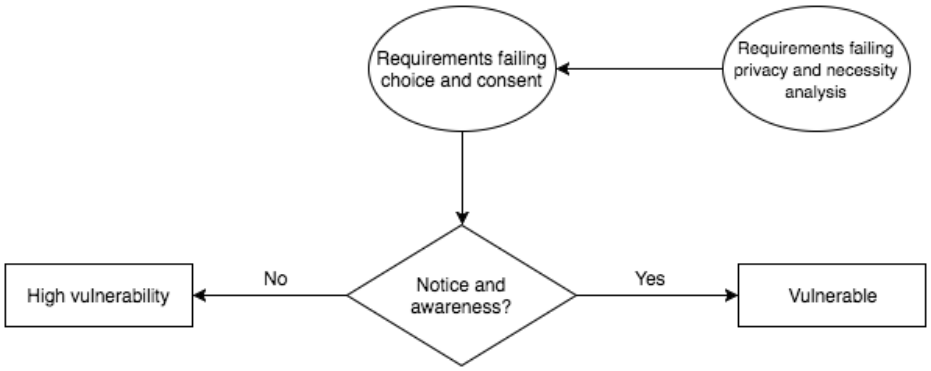

Figure 22. Notice and awareness

If requirements fail in providing privacy by default, choice and consent and use users PII, then the they can only be classified as either highly vulnerable or vulnerable requirements. Requirements must still provide notice and awareness to the user, so that the user could reverse the actions. For instance, a user tagged in someone else's picture, the user is notified and has an option to revert the tag. Some requirements suggest background data collection without notifying the user, such as Requirement 6.4 (collect browsing patterns of the user off the service) [Appendix B], hence they are classified as highly vulnerable requirements to the user privacy.

5.2 Vulnerability analysis

Using the guideline presented in section 5.1.2, each of vulnerability category highlighted in Table 4 can be analysed to reduce and rate the vulnerable requirements. The process of eliminating vulnerable requirements is applied once privacy vulnerabilities and privacy protection goals, or in this context, requirements, have been identified. The vulnerability reduction flow illustrated in Figure 20, Figure 21, and Figure 22 were structured after analysing privacy paradigms, studying extracted vulnerability requirements and results from conducted interviews and questionnaires.

Process to identify high, low and vulnerable requirements and eliminating privacy requirements from vulnerability list shall be applied to each requirement classified as a vulnerability.

5.2.1 Information monitoring goals

A User may be monitored by Facebook by using several techniques. The most common way to monitor a user on a web service is using cookies [Acar *et al*, 2015]. A user who visits Facebook gets a cookie placed in his/her browser with a lifetime of two years [Acar *et al*, 2015], along with some other cookies which hold varying information, as elaborated in Table 11.

Name	Sample value	Contains	Expires	Secure?

c_user	100004223456398	User id	Session/ 1Month	Yes
datr	S3fJVgeTh7_ikK5frtHsHPmE	Browser ID	2 years	No
fr	0goRJJKaszKOLdKz8.AWXGHlRrxSL M3P HeHxfrORvl0H8.BCVChV.Sj.FUJ.0. AW WSuv8a	Encrypted facebook id and browser id	1 Month	No
lu	100004223456398	Encrypted id of last user	2 years	Yes
P	-2	User channel partitions	Session	No
Presence	EM426705095EuserFA21B092112 98286 A2EstateFDutF1426705095426Et 2F	Chat state	Session	Yes
xs	244%3AjlZKp45fK9ceMA%3A2%3 A14267 05088%3A3455	Session number and secret	Session	Yes
Act	1426704200575%2F14	Timestamp and counter of user actions	Session	No

Table 11. Cookie usage of Facebook [Acar et al, 2015]

These cookies are placed and read every time a user visits Facebook and a web service that utilizes Facebook API [Acar, *et al*, 2015], regardless of user state (logged in or logged out). Individual monitoring requirements may be subjected to following heuristics to determine if they are actually vulnerable.

Requirement 2.15 highlights synchronization of contacts and browsing history from user's devices. While the system must check hardware permissions before accessing this information, the prevention is off service and set by user on his/her device. Furthermore, post-conditions and sub-goals associated with the requirement suggest that the information is used to suggest new friends to the user and provide relevant advertisements to the user, both exhibiting vulnerability characteristics. Lastly, when contacts and browsing history is synchronized [O'Reilly, 2011], the system fails to notify users of such action and hence it is considered to be a highly vulnerable requirement.

After vulnerability analysis, Requirement 2.4 was eliminated from vulnerability list, requirement 2.6, 2.15, 5.1 and 8.1 were categorized as highly vulnerable requirements due to their failure to provide choice and consent and absence of user

awareness, whereas, requirements 8.2 and 8.10 are considered vulnerable as they may affect user and users' friend privacy.

5.2.2 Information aggregation goals

Information shared by the user is collected, stored and used by social networking services. Sometimes, information may be aggregated to provide useful information to the user or to provide new features. Aggregation may sometime be used to hide PII, as highlighted by Requirement 6.8. However, aggregation has some issues associated with them, consider following scenario where data set is.

- There are 10 users, 8 males and 2 females.
- There are 8 users' who study at university of Tampere.
- None of the females in dataset study at university of Tampere.

If it is known that a male user is part of the dataset, it can be inferred that the specific user studies at university of Tampere. Facebook utilizes The object and association (TAO) to serve data over graph API. The association method works identically to the scenario presented above.

From privacy vulnerabilities classified as information aggregation requirements, Requirement 5.3 highlights aggregation of stored pictures to suggest automatic tags to user. There is a privacy feature associated with the functionality which is represented by Requirement 3.29, however, user must enable this functionality, and if this functionality is disabled, the vulnerability may affect user and their friends' privacy. Because if this reason Requirement 5.3 is vulnerable but vulnerability is low since functionality provides consent and privacy setting, but uses personal information and failure of privacy setting will affect user and his/her friends' privacy.

Requirement 6.10 suggests Facebook receives information from third party services about users' browsing patters. Facebook then aggregates the information to provide relevant advertisements on users' time line. The function does not provide value to user, instead, it provides value to the business and it also fails to provide security features and fails to acquire user consent along with notice and awareness, hence the feature is highly vulnerable. Out of three requirements in the category of information aggregation, Requirement 5.3 posses a relatively low threat to user privacy, whereas requirements 6.5 and 6.10 are highly vulnerable to user privacy.

5.2.3 Information storage goals

Facebook may store user information upon user consent, however, the user has little control of what happens afterwards. Because of the elasticity of cloud storage and computing, the data might be relocated into several server(s) to ensure availability and

maintain integrity [Chen *et al*, 2012]. The three key aspects of data storage are data integrity, data confidentiality and data availability. While data availability is dealt with making several copies of user data, data confidentiality and data integrity are users' major concerns. However, some of the requirements listed as vulnerabilities and under the category information storage may be crucial to provide functionality to user. Moreover, according to study conducted by [Vail *et al*, 2008], information storage may not be one of the top concern for an online user. Based on this information, several assessments were made to exclude and categorize storage vulnerabilities.

Considering Requirement 2.5 (Store login time and date), the requirement exhibits similar behavior as Requirement 2.4 for information monitoring. Requirement 2.5 contributes significantly in providing security features highlighted by Requirement 2.17, where a security feature is a pre-condition, post-condition, constraint, or an obstacle preventing achievement of a requirement. As Requirement 2.17 is a security features which may require Requirement 2.5, it is safe to eliminate Requirement 2.5 from the list. Another example of elimination can be taken from Requirement 1.4, where user name, email, date of birth and gender of user are stored, however, these attributes provide crucial functionality to the user and can be eliminated from list of vulnerabilities.

Requirement 10.2 suggests that Facebook may retain information of deleted Facebook account to provide features to active users. Implications associated with the requirements may be severe and stands against one of the concept of privacy, right to be forgotten. For this reason, Requirement 10.2 is highly vulnerable to user privacy.

Requirements 1.4, 2.10, 2.14, 3.3, 3.8, 3.12, 3.16, 3.20, 3.24, 3.39 were eliminated. Requirements 4.9 and 4.11 are considered less threatening to user privacy, whereas Requirements 3.40, 10.2 and 3.41 prove to be highly vulnerable to users' privacy. Truest is really important when it comes to information storage, [Zhou *et al*, 2010] believes that people prefer storing their data on private devices rather than cloud storage.

5.2.4 Information transfer goals

According to Vail *et al* [2008], information transfer is the top most concern of internet users'. Users' are uncomfortable if their information is transferred, sold, or shared without them being notified. Information may be transferred to partner companies and vendors in one or more ways. Cookies may be used to transfer browsing information whereas partner companies may be granted direct access to user data. Developers may be granted access to user data, statistics may be sent advertisements statistics or vendors may receive user private information or perhaps even law enforcement authorities.

Requirement 6.9 states that advertisement statistics may be transferred to advertisers to monitor out reach and improve advertisement services. Although the functionality does not provide any valuable functionality to the user, Requirement 6.8 provides a security measure which highlights aggregation of statistics to hide personal

information and hence it can be eliminated from the list. Requirement 5.7 suggests user information will be transferred to vendors, partners and service providers and no privacy preserving requirements are highlighted which may obstruct the requirement from being achieved and hence it is classified as a highly vulnerable functionality.

Facebook also provides developers with a feature, Facebook single sign on. The feature allows developers to access user information, that information may or may not be private. However, since there is a chance that transferred information is private, the feature is still considered vulnerable to user privacy. However, Requirement 9.3 suggests that application making use of personal user information will be reviewed by Facebook themselves to make sure implementation follows policies of Facebook Once the application is reviewed, Requirement 9.7 makes sure no information is transferred without consent of user, for this reason, requirements 9.9 - 9.17 are less vulnerable to users' as compared to other features on Facebook. Although, it is expected of web services to exchange personal information [Schrader, 1991] it is essential that provider asserts secure transmission of data or avoid it altogether.

5.2.5 Information collection goals

A social networking service may have several reasons to collect information from user. Collection can be done in order to provide functionality and service to user, which is usually direct collection. On a contrast, indirect collection may also take place for organizational benefits.

Information collection requirements on Facebook are consistent with information storage requirements such as Requirement 2.13 from information collection and Requirement 2.14 of information storage. Since Requirements 2.13, 3.2, 3.7, 3.11, 3.15, 3.19, 3.23, 4.8, 4.10 highlight collection of data from user. Collection highlighted by these requirements are direct collection i.e. with consent of the user and user is aware information is being collected. Furthermore, collection of attributes represented by these foals are necessary to provide functionality to the user. These requirements can be eliminated from the list to narrow down the subset of vulnerabilities.

Requirement 6.4 explains a scenario where users' browsing patterns are monitored off the service. Collection of browsing patterns off the service happens without consent of user, provides one added functionality where users' age can be monitored (Vulnerability) and hence Requirement 6.4 is considered a highly vulnerable feature. Similarly, Requirement 5.2 also represents a highly vulnerable functionality.

5.2.6 Information personalization goals

User information may be used by social networking service to provide new features. Problem with information personalization is that user information is taken out of context. Features like searching and suggestions based on users' content are two of the most ways

user data can be used to provide new features. For searching, there are two major privacy concerns: how queries are related and what private information is handled by the query [Xiong, 2007].

Facebook may synchronize contacts from user device to suggest new friends to the user, where the feature is associated with no system privacy preserving mechanism and hence it is highly vulnerable. Similarly, Facebook may use all available information to provide search feature (Figure 6). Information such as users' telephone number may be used to search users on Facebook and user can iterate through numbers which will yield a profile of searched user along with other publically available information. This makes Requirement 7.1 highly vulnerable as well. Requirement 2.7 is considered to have low vulnerability, Requirements 5.4 and 5.5 are vulnerable whereas Requirements 5.6 and 7.1 are highly vulnerable.

5.3 Results

Analyzing Facebooks' policies, terms and conditions, and other documents with GBRAM resulted in extraction of 155 initial requirements which, after refinement were reduced to 136. The goal set contains 44 maintenance requirements and 92 achievement requirements. 95 requirements exhibiting privacy associated functionalities were extracted from the goal set whereas the rest are eliminated. Out of 95, 40 requirements highlight privacy protection requirements whereas 55 requirements suggest privacy vulnerabilities.

The number of vulnerabilities did not fairly represent security features Facebook provides to maintain privacy of user while using the service, hence, a method was suggested based on interviews conducted [Appendix C] to minimize number of privacy vulnerabilities. Privacy vulnerabilities when studied under vulnerability analysis reduced vulnerability goal set by 21 requirements. Information storage was reduced the most by 12 requirements since storing information is somewhat necessary to provide users with functionality over Facebook. Furthermore, the eliminated information storage requirements allowed users to modify and delete existing information, except storage of friend list, a full list of requirements eliminated from privacy vulnerability category are listed in Table 12.

Requirement	Description	Eliminated at phase
Requirement 1.4	Store name, email, date of birth and gender	1st phase
Requirement 2.4	Monitor login activity of active account	1st phase
Requirement 2.5	Store login time and date	1st phase
Requirement 2.10	Store location at login	1st phase
Requirement 2.13	Collect hardware and network information	1st phase
Requirement 2.14	Store operating system information and device types	1st phase
Requirement 3.2	Collect created statuses	1st phase

Requirement 3.3	Store created status	1st phase
Requirement 3.7	Collect created photo, video	1st phase
Requirement 3.8	Store created phot, video	1st phase
Requirement 3.11	Collect users liked objects	1st phase
Requirement 3.12	Store users' liked object	1st phase
Requirement 3.15	Collect conversations sent or received	2nd phase
Requirement 3.16	Store conversations sent or received	2nd phase
Requirement 3.19	Collect new check-in or tagged check-in	2nd phase
Requirement 3.20	Store user created check-in	2nd phase
Requirement 3.23	Collect information of friend that user added	2nd phase
Requirement 3.24	Store information of added friend	2nd phase
Requirement 3.39	Store time and date of content creation	1st phase
Requirement 4.8	Collect credit/debit card number provided by user	2nd phase
Requirement 4.10	Collect shipping, billing information provided by user	1st phase

Table 12. Requirements eliminated from vulnerability classification

Off service monitoring is perhaps the biggest vulnerability on Facebook, with features like storing browsing history, receiving browsing information and monitoring user age and synchronizing contacts from user device highlighting lack of user control over these vulnerabilities [O'Reilly, 2011]. Information aggregation is another aspect in which Facebook fails to deliver security to user, however, Facebooks' TAO works with associations which works on the principle of aggregation.

A lot of privacy settings are provided to user on Facebook, however, Facebook fails to provide privacy by default to the user and user must do a lot to make sure his/her private information remains secure. Another issue that was highlighted by this study is the extensiveness of data ownership. Facebook is designed as such that whoever can view any content, is the rightful owner of it, perhaps, this statement is true for all web services, however, context of data shared on Facebook may be more private [Barker *et al*, 2009]. Amongst the principles of privacy discussed in Chapter 3, Facebook also fails at 'right to be forgotten' since user data may be retained, transferred or shared with authorities, vendors and service providers. However, after vulnerability analysis, a lot of vulnerabilities were eliminated from the goal set and security features provided by Facebook may be sufficient to maintain user privacy.

6. Conclusion, limitations and future work

Goal based requirements analysis method provides an excellent way to enlist requirements from set of policies and other available documents. The output depends on how well an analyst understands the system being analyzed, because of this reason, different analysts may have different set of output requirements. For that reason, GBRAM method is as good as an analyst.

GBRAM method can be used to analyze requirements for any system which at least lists its requirements online. GBRAM along with privacy taxonomy suggested by Anton and Earp is an effective way of analyzing privacy requirements and also categorizing requirements as either vulnerability requirements or privacy protection requirements.

Privacy vulnerability requirements are categorized further into 7 categories, while the original authors applied the framework on health systems which are responsible for collecting and storing patient health data, this thesis applied the methodology to SNS systems, more specifically Facebook. It was determined that requirements in some categories were unjustly listed as privacy vulnerabilities, specifically storage and collection categories. Since social networking services require to collect and store user data, there are always going to be vulnerabilities according to privacy taxonomy.

A method was proposed as a contribution for eliminating and classifying vulnerabilities. The vulnerability analysis method required analyst to ask four questions.

- Privacy association
- Necessity of functionality
- Choice and consent
- Value to user

These four points were highlighted by interviewees which helped to determine under what circumstances was it okay to monitor, aggregate, store, collect, transfer, personalize and contact using users' data. While privacy association, necessity of functionality and choice and consent helps to eliminate vulnerabilities from the goal set, if a goal does not provide any of the above three functionalities, a goal would remain vulnerable. From there it is determined whether a goal is Highly vulnerably, has medium vulnerability or whether the vulnerability is low using principles of privacy paradigms discussed in chapter 3.

As stated earlier, the resultant goal set using the GBRAM method would always differ from one analyst to another, which is perhaps its limitation and its positive aspect as well as different sets of functionalities and eventually vulnerabilities would be discovered. The method can be applied to any available system; however, it can be improved. A domain specific language can be made to support GBRAM and privacy taxonomy established by Anton and Earp (2004) furthermore, vulnerability analysis can then be applied to determine how vulnerable a certain goal is.

7. References

[Abril and Lipton, 2014] "Right to Be Forgotten: Who Decides What the World Forgets, The", *Ky.LJ,* vol. 103, pp. 363.

[Acar *et al,* 2015] *Facebook tracking through social plug-ins*, iMinds.

[*Adar et al,* 1999] "Haystack: Per-user information environments", *Proceedings of the eighth international conference on Information and knowledge management*ACM, , pp. 413.

[Albarran, 2013] *The social media industries,* Routledge.

[Altshuler *et al,* 2012] *Security and privacy in social networks,* Springer Science & Business Media.

[Anton, 1997] "Goal identification and refinement in the specification of software-based information systems", .

[*Anton,* 1996] "Goal-based requirements analysis", *Requirements Engineering, 1996., Proceedings of the Second International Conference on*IEEE, , pp. 136.

[Anton and Earp, 2004] "A requirements taxonomy for reducing web site privacy vulnerabilities", *Requirements Engineering,* vol. 9, no. 3, pp. 169-185.

[*Antón et al,* 2000] "Strategies for developing policies and requirements for secure electronic commerce systems", *E-commerce security and privacy*Citeseer, , pp. 29.

[*Antón et al,* 2001] "The role of policy and stakeholder privacy values in requirements engineering", *Requirements Engineering, 2001. Proceedings. Fifth IEEE International Symposium on*IEEE, , pp. 138.

[API, 2015] October17, 2015-last update, *Facebook common api endpoints* [Homepage of Facebook], [Online]. Available: https://developers.facebook.com/docs/graph-api/reference/user [2016, 04/06].

[Arbaugh *et al,* 2000] "Windows of vulnerability: A case study analysis", *Computer,* vol. 33, no. 12, pp. 52-59.

[Barker *et al,* 2009] "A data privacy taxonomy" in *Dataspace: The Final Frontier* Springer, , pp. 42-54.

[Bartlett and Burt, 1933] "Remembering: A study in experimental and social psychology", *British Journal of Educational Psychology,* vol. 3, no. 2, pp. 187-192.

[*Beaver et al,* 2010] "Finding a Needle in Haystack: Facebook's Photo Storage.", *OSDI*, pp. 1.

[Bennett, 2012] "Right to be forgotten: Reconciling eu and us perspectives, the", *Berkeley J. Int'l L.,* vol. 30, pp. 161.

[*Borthakur et al,* 2011] "Apache Hadoop goes realtime at Facebook", *Proceedings of the 2011 ACM SIGMOD International Conference on Management of data*ACM, , pp. 1071.

[Boyd and Ellison, 2010] "Social network sites: definition, history, and scholarship", *IEEE Engineering Management Review,* vol. 3, no. 38, pp. 16-31.

[Cashmore, 2009] 19/09/2009-last update*, Rip facebook beacon* [Homepage of Mashable], [Online]. Available: http://mashable.com/2009/09/19/facebook-beacon-rip/#_ZwZxs.DpPqr [2016, 04/03].

[Cavoukian and Chanliau, 2013] "Privacy and security by design: a convergence of paradigms", *Ontario, Canada: Office of the Privacy Commissioner (Ontario),* .

[*Chen et al,* 2012] "Data security and privacy protection issues in cloud computing", *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*IEEE, , pp. 647.

[Cookies, 2015] 20 Jan 2015-last update [Homepage of Facebook Inc], [Online]. Available: https://www.facebook.com/help/cookies/ [2016, 04/20].

[Cottrill, 2014] "Privacy in context: an evaluation of policy-based approaches to location privacy protection", *International Journal of Law and Information Technology,* vol. 22, no. 2, pp. 178-207.

[Culnan, 1999] "Georgetown internet privacy policy survey: report to the federal trade commission", *Washington, DC: Georgetown University, The McDonough School of Business,* .

[Curtiss *et al,* 2013] "Unicorn: A system for searching the social graph", *Proceedings of the VLDB Endowment,* vol. 6, no. 11, pp. 1150-1161.

[*Cvijikj et al,* 2011] "Monitoring trends on facebook", *Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on*IEEE, , pp. 895.

[Data, 2015]*, Accessing your facebook data* [Homepage of Facebook], [Online]. Available: https://www.facebook.com/help/405183566203254/ [2016, 04/06].

[Dwyer *et al,* 2007] "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace", *AMCIS 2007 proceedings,* , pp. 339.

[Edwards and Brown, 2009] "Data Control and Social Networking: Irreconcilable Ideas?", *LAW AND THE FUTURE OF DATA CONTROL.Data Control and Social Networking: Irreconcilable Ideas?* vol. 23.

[Eecke, 2014] "Privacy by Design Privacy by Default Legal Concepts", .

[Freudiger *et al,* 2011] "Evaluating the privacy risk of location-based services" in *Financial Cryptography and Data Security* Springer, , pp. 31-46.

[Gantz and Reinsel, 2012] "The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east", *IDC iView: IDC Analyze the future,* vol. 2007, pp. 1-16.

[Griffiths and Remenyi, 2008] "Aligning knowledge management with competitive strategy: A framework", *The Electronic Journal of Knowledge Management,* vol. 6, no. 2, pp. 125-134.

[*Gross et al,* 2005] "Information revelation and privacy in online social networks", *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*ACM, , pp. 71.

[Jansen and Grance, 2011] "Guidelines on security and privacy in public cloud computing", , pp. 1.

[Johnson *et al,* 2012] "Facebook and its privacy: its complicated" in *Proceedings of the Eighth Symposium on Usable Privacy and Security* ACM, , pp. 1-9.

[*Kabir et al,* 2009] "Conditional Purpose Based Access Control Model for Privacy Protection", *Proceedings of the Twentieth Australasian Conference on Australasian Database-Volume 92. Australian Computer Society, Inc.*Australia.

[*Karjoth et al,* 2002] "A privacy policy model for enterprises", *Computer Security Foundations Workshop, 2002. Proceedings. 15th IEEE*IEEE, , pp. 271.

[*Kavakli et al,* 2003] "Goal driven requirements engineering: evaluation of current methods", *Proceedings of the 8th CAiSE/IFIP8*, pp. 16.

[Khanna, "Facebook's Privacy Incident Response: a study of geolocation sharing on Facebook Messenger", .

[Kristol, 2001] "HTTP Cookies: Standards, privacy, and politics", *ACM Transactions on Internet Technology (TOIT),* vol. 1, no. 2, pp. 151-198.

[Lapouchnian, 2005] "Goal-oriented requirements engineering: An overview of the current research", *University of Toronto,* , pp. 32.

[LeBlanc, 2011] *Programming Social Applications: Building Viral Experiences with OpenSocial, OAuth, OpenID, and Distributed Web Frameworks,* " O'Reilly Media, Inc.".

[*Lichtenstein,* 1997] "Developing Internet security policy for organizations", *System Sciences, 1997, Proceedings of the Thirtieth Hawaii International Conference on*IEEE, , pp. 350.

[*Liu et al,* 2003] "Security and privacy requirements analysis within a social setting", *Requirements Engineering Conference, 2003. Proceedings. 11th IEEE International*IEEE, , pp. 151.

[Malhotra *et al,* 2004] "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model", *Information Systems Research,* vol. 15, no. 4, pp. 336-355.

[Mark, 2013] *, Tao, the power of graph*. Available: https://www.facebook.com/notes/facebook-engineering/tao-the-power-of-the-graph/10151525983993920 [2015, November/23].

[Mayer *et al,* 1995] "An integrative model of organizational trust", *Academy of management review,* vol. 20, no. 3, pp. 709-734.

[McFarland, 2012] "What is privacy" in Santa Clara University, .

[Mishra and Crampton, 1998] "Employee monitoring: privacy in the workplace?", *SAM Advanced Management Journal,* vol. 63, no. 3, pp. 4.

[O'Reilly, 2011] "Facebook technical analysis report" in O'Reilly, , pp. 153.

[Policy, 2015] January 30-last update*, Facebook data policy* [Homepage of Facebook], [Online]. Available: https://www.facebook.com/about/privacy/ [2016, 04/06].

[Polonetsky, 2013] *An Updated Privacy Paradigm for the "Internet of Things",* 1-5.

[Prigg, 2014] 23 July 2014-last update*, Facebook now has 1.32 BILLION users* [Homepage of Daily mail], [Online]. Available: http://www.dailymail.co.uk/sciencetech/article-2703440/Theres-no-escape-Facebook-set-record-stock-high-results-beats-expectations-1-32-BILLION-users-30-mobile.html [2016, 04/06].

[Rappa, 2003] "Business models on the web", *Available at Managing the Digital Enterprise website: http://digitalenterprise.org*, .

[Richards and King, 2014] "Big data ethics", *Wake Forest L.Rev.,* vol. 49, pp. 393.

[Rights, 2015] 30 january 2015-last update*, Statement of rights* [Homepage of Facebook Inc.], [Online]. Available: https://www.facebook.com/legal/terms [2016, 04/20].

[Schrader, 1991] "Informal technology transfer between firms: Cooperation through information trading", *Research policy,* vol. 20, no. 2, pp. 153-170.

[Schwartz and Ward, 2004] "Doing better but feeling worse: The paradox of choice", *Positive psychology in practice,* , pp. 86-104.

[Sullivan, 2011] "Study: Social media polarizes our privacy concerns", *MSNBC.Retrieved March,* vol. 24, pp. 2012.

[Traverso, 2013] "Presto: Interacting with petabytes of data at Facebook", *Retrieved February,* vol. 4, pp. 2014.

[Vail *et al,* 2008] "An empirical study of consumer perceptions and comprehension of web site privacy policies", *Engineering Management, IEEE Transactions on,* vol. 55, no. 3, pp. 442-454.

[Volakis, 2011] *Trust in Online Social Networks,* .

[Westin, 2003] "Social and political dimensions of privacy", *Journal of Social Issues,* vol. 59, no. 2, pp. 431-453.

[Wheeler, 2013] "Introduction to Apache Hadoop".

[Wiegers and Beatty, J., 2013] *Software requirements,* Pearson Education.

[*Xiong et al,* 2007] "Towards privacy-preserving query log publishing", *Query Log Analysis: Social and Technological Challenges. A workshop at the 16th International World Wide Web Conference (WWW 2007)* May, .

[*Zhou et al,* 2010] "Security and privacy in cloud computing: A survey", *Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on*IEEE, pp. 105.

Appendix A

Policy 1 description:
We collect the content and other information you provide when you use our Services, including when you sign up for an account, create or share, and message or communicate with others. This can include information in or about the content you provide, such as the location of a photo or the date a file was created. We also collect information about how you use our Services, such as the types of content you view or engage with or the frequency and duration of your activities.

Policy 2 description:
We also collect content and information that other people provide when they use our Services, including information about you, such as when they share a photo of you, send a message to you, or upload sync or import your contact information.

Policy 3 description:
We collect information about the people and groups you are connected to and how you interact with them, such as the people you communicate with the most or the groups you like to share with.

Policy 4 description:
If you use our Services for purchases or financial transactions (like when you buy something on Facebook, make a purchase in a game, or make a donation), we collect information about the purchase or transaction. This includes your payment information, such as your credit or debit card number and other card information, and other account and authentication information, as well as billing, shipping and contact details.

Policy 5 description:
We collect information from or about the computers, phones, or other devices where you install or access our Services, depending on the permissions you have granted. We may associate the information we collect from your different devices, which helps us provide consistent Services across your devices. Here are some examples of the device we collect:

- Attributes such as the operating system, hardware version, device settings, file and software names and types, battery and signal strength, and device identifiers.
- Device locations, including specific geographic locations, such as through GPS, Bluetooth, or Wi-Fi signals.

- Connection information such as the name of your mobile operator or ISP, browser type, language and time zone, mobile phone number and IP address.

Policy 6 description:
We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button or Facebook Log In or use our measurement and advertising services). This includes information about the websites and apps you visit, your use of our Services on those websites and apps, as well as information the developer or publisher of the app or website provides to you or us.

Policy 7 description:
We receive information about you and your activities on and off Facebook from third-party partners, such as information from a partner when we jointly offer services or from an advertiser about your experiences or interactions with them.

Policy 8 description:
We receive information about you from companies that are owned or operated by Facebook, in accordance with their terms and policies.

Policy 9 description:
We also use information we have to provide shortcuts and suggestions to you. For example, we are able to suggest that your friend tag you in a picture by comparing your friend's pictures to information we have put together from your profile pictures and the other photos in which you have been tagged. If this feature is enabled for you, you can control whether we suggest that another user tag you in a photo using the “Timeline and Tagging” settings.

Policy 10 description:
When we have location information, we use it to tailor our Services for you and others, like helping you to check-in and find local events or offers in your area or tell your friends that you are nearby.

Policy 11 description:
We use your information to send you marketing communications, communicate with you about our Services and let you know about our policies and terms. We also use your information to respond to you when you contact us.

Policy 12 description:
We use the information we have to improve our advertising and measurement systems so we can show you relevant ads on and off our Services and measure the effectiveness and reach of ads and services.

Policy 13 description:
We use the information we have to help verify accounts and activity, and to promote safety and security on and off our Services, such as by investigating suspicious activity or violations of our terms or policies. We work hard to protect your account using teams of engineers, automated systems, and advanced technology such as encryption and machine learning.

Policy 14 description:
When you share and communicate using our Services, you choose the audience who can see what you share. For example, when you post on Facebook, you select the audience for the post, such as a customized group of individuals, all of your Friends, or members of a Group. Likewise, when you use Messenger, you also choose the people you send photos to or message.

Policy 15 description:
Public information is available to anyone on or off our Services and can be seen or accessed through online search engines, APIs, and offline media, such as on TV.

Policy 16 description:
In some cases, people you share and communicate with may download or re-share this content with others on and off our Services. When you comment on another person's post or like their content on Facebook, that person decides the audience who can see your comment or like. If their audience is public, your comment will also be public.

Policy 17 description:
When you use third-party apps, websites or other services that use, or are integrated with, our Services, they may receive information about what you post or share. For example, when you play a game with your Facebook friends or use the Facebook Comment or Share button on a website, the game developer or website may get information about your activities in the game or receive a comment or link that you share from their website on Facebook. In addition, when you download or use such third-party services, they can access your Public Profile, which includes your username or user ID, your age range and country/language, your list of friends, as well as any information that you share with

them. Information collected by these apps, websites or integrated services is subject to their own terms and policies.

Policy 18 description:
We share information we have about you within the family of companies that are part of Facebook. Learn more about our companies.

Policy 19 description:
If the ownership or control of all or part of our Services or their assets changes, we may transfer your information to the new owner.

Policy 20 description:
We do not share information that personally identifies you (personally identifiable information is information like name or email address that can by itself be used to contact you or identifies who you are) with advertising, measurement or analytics partners unless you give us permission.

Policy 21 description:
We transfer information to vendors, service providers, and other partners who globally support our business, such as providing technical infrastructure services, analyzing how our Services are used, measuring the effectiveness of ads and services, providing customer service, facilitating payments, or conducting academic research and surveys. These partners must adhere to strict confidentiality obligations in a way that is consistent with this Data Policy and the agreements we enter into with them.

Policy 22 description:
You can also download information associated with your Facebook account through our Download Your Information tool.

Policy 23 description:
We store data for as long as it is necessary to provide products and services to you and others, including those described above. Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services.

Policy 24 description:
Information that others have shared about you is not part of your account and will not be deleted when you delete your account.

Policy 25 description:
We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards.

Policy 26 description:
We also may retain information from accounts disabled for violations of our terms for at least a year to prevent repeat abuse or other violations of our terms.

Policy 27 description:
We will notify you before we make changes to this policy and give you the opportunity to review and comment on the revised policy before continuing to use our Services.

Policy 28 description:
We may use cookies to help protect your account from being accessed by anyone other than you. Cookies and similar technologies also let us know when several people have logged in from the same computer. They (cookies) also help us implement login notifications, so you can be alerted when your account is accessed and disable any active sessions.

Policy 29 description:
Besides helping to keep unauthorized people from logging into your account, we also use Cookies and similar technologies to help make sure the people or machines that access our Services don't violate our policies. We may also use a cookie to learn whether someone who was served an ad on Facebook Services later makes a purchase on the advertiser's site or installs the advertised app.

Policy 30 description:
We may store information in a cookie that is placed on your browser or device so you will see the site in your preferred language.

Policy 31 description:
Cookies or similar technologies help you log in by pre-filling the username field and help make chat a better experience by showing which of your friends are online.

Policy 32 description:
For example, we may use Cookies or similar technologies to help us route traffic between servers and understand how quickly Facebook Services load for different people.

Policy 33 description:
Identify and disable the accounts of spammers by monitoring cookies of users and non-users of Facebook.

Policy 34 description:
Prevent people who are underage from signing up with a false birth date by monitoring users filed forms on and off service.

Policy 35 description:
Identify public computers so that we can discourage people from using **Keep me logged in** and putting their account at risk

Policy 36 description:
You own all of the content and information you post on Facebook and you can control how it is shared through your privacy and application settings.

Policy 37 description:
- You grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless content has been shared with others, and they have not deleted it.
- Removed content may persist in backup copies for a reasonable period (but will not be available to others).
- When you publish content or information using the Public setting, it means that you are allowing everyone, including people off Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).

Policy 38 description:
- You will not post unauthorized commercial communications (such as spam) on Facebook.
- You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission.
- You will not bully, intimidate, or harass any user.
- You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory.

- You will not do anything that could disable, overburden, or impair the proper working or appearance of Facebook, such as a denial of service attack or interference with page rendering or other Facebook functionality.
- You will not facilitate or encourage any violations of this Statement or our policies.

Policy 39 description:

Facebook Login lets people quickly and easily create an account in your app without having to set (and likely later forget) a password. Developers can access public_profile, user_friends and email without submitting application for a review from facebook.

Policy 40 description:

Policy 40 enlists relevant graph search API action points to this study. These actions represent the API functionalities that are available for developers. Developers may choose to gather user data from at least following end points.

- A user access token with user_games_activity permission, for any achievements that person has made in any app.
- A user access token with user_photos permission to retrieve any albums that the session user has uploaded.
- To read a comment, you generally need the same permissions as required for viewing the object that the comment was added to.
- A Page access token with read_page_mailbox permission is required.
- A user access token with user_events permission can be used to retrieve any events that are visible to that person
- A user access token with read_custom_friendlists permission is required.
- The user_managed_groups permission can be used to read the group content for a group in which the user is an admin. This permission also allows the app to post as the user in the group if the app is also granted the publish_actions permission.
- The same permissions required to view the parent object are required to view likes on that object.
- A user access token with user_posts permission, for someone who is able to view the post after privacy settings are taken into account.
- An app access token for the app that created the payment is required.
- A user's videos can be read if the owner has granted the user_videos or user_postspermission.

Policy 41 description:

These are the categories of Facebook data that are available to you either in your activity log or your downloaded data, or in both places [Data, 2015].

Appendix B

Goal 1: Account signup activities:

Activities that a user or a system may perform have been divided into several categories, among witch, the first step is account signup activities. A new user on facebook would try to create account and register on Facebook. The requirements have been sorted according to their precedence and functionalities suggested are as follows.

Requirement 1.1:	Prevent multiple accounts from same user
Policy:	1
Type:	Maintenance
Action:	Prevent account creation
Agent:	System
Stakeholder:	User, System
Constraints:	User creates a duplicate account or violates privacy
Obstacles:	No duplicities found (Contract failure)
Pre-condition:	-
Post-condition:	User prevented from creating account
Sub goals:	-

Requirement 1.2:	Create account
Policy:	1
Type:	Achievement
Action:	Account signup
Agent:	User
Stakeholder:	User, System
Constraints:	User signs up for a new account
Obstacles:	User account already exists (Contract failure)
Pre-condition:	Requirement 1.1: Prevent account creation
Post-condition:	Requirement 1.3: Provided name, email, date of birth and gender
Sub goals:	-

Requirement 1.3:	Provide name, email, date of birth and gender
Policy:	1
Type:	Achievement
Action:	Account information
Agent:	User
Stakeholder:	User, System
Constraints:	User signs up for a new account
Obstacles:	-
Pre-condition:	Requirement 1.2: Allow users to create account
Post-condition:	Requirement 1.4: Store name, email, date of birth and gender
Sub goals:	Requirement 1.6: Provide profile picture, phone number

Requirement 1.4:	Store name, email, date of birth and gender
Policy:	1
Type:	Achievement

Action:	Store signup data
Agent:	System
Stakeholder:	User, System
Constraints:	User signs up for a new account
Obstacles:	-
Pre-condition:	Requirement 1.3: Provide name, email, date of birth and gender
Post-condition:	-
Sub goals:	Requirement 10.1: Allow users to delete their account.

Requirement 1.5:	Provide profile picture, phone number
Policy:	1
Type:	Achievement
Action:	Provide additional information
Agent:	User
Stakeholder:	User, System
Constraints:	User signs up for a new account
Obstacles:	-
Pre-condition:	User provides, name, email date of birth and gender.
Post-condition:	Requirement 2.2: Account verification
Sub goals:	Requirement 10.1: Allow users to delete their account

Goal 2: Account Login activities:

Once a user has created an account or was denied account creation because of already existing account, user can log into his/her account. The steps that take place during that process are listed as functionalities below.

Requirement 2.1:	Log into existing account
Policy:	1
Type:	Achievement
Action:	Account login
Agent:	User
Stakeholder:	User, System
Constraints:	User has an existing account on facebook
Obstacles:	User does not have an account (Precedence failure Requirement 1.1)
Pre-condition:	User has an account on facebook
Post-condition:	Requirement 2.2: Account verification
Sub goals:	Requirement 10.1: Allow users to delete their account

Requirement 2.2:	Verify account at login or account creation
Policy:	1
Type:	Achievement
Action:	Verify user account
Agent:	System
Stakeholder:	User, System
Constraints:	User signs up for a new account

	User logs into an existing account
Obstacles:	User does not have an account (Precedence failure Requirement 1.2)
	Incorrect credentials entered (General failure)
Pre-condition:	-
Post-condition:	Requirement 2.3: Retrieve content
Sub-goals:	-

Requirement 2.3:	Retrieve content from user account.
Policy:	1
Type:	Achievement
Action:	Retrieve content
Agent:	System
Stakeholder:	User, System
Constraints:	Account validation successful
Obstacles:	Account does not exist (Contract failure Requirement 2.2)
	Incorrect credentials (Contract failure Requirement 2.2)
Pre-condition:	Requirement 2.1: Allow users to login
Post-condition:	Content retrieved
Sub-goals:	Requirement 2.4: Monitor login activity
	Requirement 2.6: Monitor language and region
	Requirement 2.8: Monitor location

Requirement 2.4:	Monitor login activity of active account
Policy:	28
Type:	Maintenance
Action:	Monitor login activity
Agent:	System
Stakeholder:	User, System
Constraints:	Account validation successful
Obstacles:	Account validation unsuccessful (General failure)
Pre-condition:	Requirement 2.1: Allow users to login
Post-condition:	Store login statistics
Sub-goals:	Requirement 2.5: Store login time and date.
	Requirement 2.14: Log activity to prevent unauthorized access

Requirement 2.5:	Store login time and date
Policy:	28
Type:	Achievement
Action:	Store login information
Agent:	System
Stakeholder:	User, System
Constraints:	Account validation successful
Obstacles:	Account does not exist (Contract failure Requirement 2.2)
	Incorrect credentials (Contract failure Requirement 2.2)
Pre-condition:	Requirement 2.1: Allow users to login
Post-condition:	-

Sub-goals:	Requirement 2.14: Log activity to prevent unauthorized access

Requirement 2.6:	Monitor language and region of logged in account
Policy:	30
Type:	Maintenance
Action:	Monitor language and region
Agent:	System
Stakeholder:	User, System
Constraints:	Account validation successful
Obstacles:	Account does not exist (Contract failure Requirement 2.2) Incorrect credentials (Contract failure Requirement 2.2)
Pre-condition:	Requirement 2.1: Allow users to login
Post-condition:	Requirement 2.7: Personalize profile with language and region
Sub-goals:	-

Requirement 2.7:	Personalize profile with language and region
Policy:	30
Type:	Achievement
Action:	Personalize profile
Agent:	System
Stakeholder:	User, System
Constraints:	Account validation successful
Obstacles:	Account does not exist (Contract failure Requirement 2.2) Incorrect credentials (Contract failure Requirement 2.2)
Pre-condition:	Requirement 2.1: Allow users to login
Post-condition:	-
Sub-goals:	-

Requirement 2.8:	Monitor location
Policy:	10
Type:	Maintenance
Action:	Monitor user location when content is created, photo is shared or user shares location with friend.
Agent:	System
Stakeholder:	User, System
Constraints:	User creates, shares content.
Obstacles:	Account does not exist (Contract failure Requirement 2.2) Incorrect credentials (Contract failure Requirement 2.2)
Pre-condition:	Requirement 2.1: Allow users to login
Post-condition:	Verify rights to monitor location
Sub-goals:	Requirement 2.10: Store location at login

Requirement 2.9:	Verify rights to monitor location
Policy:	10
Type:	Achievement
Action:	Verify rights
Agent:	System

Stakeholder:	User, System
Constraints:	Account validation successful
Obstacles:	Account does not exist (Contract failure Requirement 2.2) Incorrect credentials (Contract failure Requirement 2.2)
Pre-condition:	Requirement 2.1: Allow users to login
Post-condition:	Requirement 2.10: Store location at login
Sub-goals:	Requirement 2.11: Allow users to OPT-OUT of location monitoring

Requirement 2.10:	Store location at login
Policy:	10
Type:	Achievement
Action:	Store user location
Agent:	System
Stakeholder:	User, System
Constraints:	System granted rights to get location
Obstacles:	Rights not granted (Contract failure Requirement 2.9)
Pre-condition:	Requirement 2.1: Allow users to login
Post-condition:	-
Sub-goals:	Requirement 2.14: Log activity to prevent unauthorized access

Requirement 2.11:	OPT-OUT of location monitoring
Policy:	10
Type:	Achievement
Action:	OPT-OUT of service
Agent:	User
Stakeholder:	User, System
Constraints:	User verified into account
Obstacles:	Unable to verify account (Contract failure Requirement 2.2)
Pre-condition:	Requirement 2.1: Allow users to login
Post-condition:	OPT-OUT of location monitoring
Sub-goals:	-

Requirement 2.12:	Check hardware permission to read hardware info
Policy:	5
Type:	Achievement
Action:	Check hardware access permission
Agent:	System
Stakeholder:	User, System
Constraints:	Account validation successful
Obstacles:	Account does not exist (Contract failure Requirement 2.2) Incorrect credentials (Contract failure Requirement 2.2)
Pre-condition:	Requirement 2.1: Allow users to login
Post-condition:	Requirement 2.13: Collect operating system info, device settings, software names and types, IP address.
Sub-goals:	Requirement 2.15: Synchronize contacts, browser information and browser history from user device.

Requirement 2.13:	Collect operating system info, device settings, software names and types, IP address.
Policy:	5
Type:	Achievement
Action:	Collect hardware information
Agent:	System
Stakeholder:	User, System
Constraints:	Hardware permission granted
Obstacles:	Hardware permission not granted (General failure) Account validation failed (Contract failure Requirement 2.2)
Pre-condition:	Requirement 2.1: Allow users to login
Post-condition:	Requirement 2.14: Store operating system information, device settings, software names and types, IP address.
Sub-goals:	Requirement 2.16: Log activity to prevent unauthorized access

Requirement 2.14:	Store operating system information, device settings, software names and types, IP address.
Policy:	5
Type:	Achievement
Action:	Store hardware information
Agent:	System
Stakeholder:	User, System
Constraints:	Hardware permission granted
Obstacles:	Hardware permission not granted (General failure) Account validation failed (Contract failure Requirement 2.2)
Pre-condition:	Requirement 2.1: Allow users to login
Post-condition:	-
Sub-goals:	-

Requirement 2.15:	Synchronize contacts, browser information and browser history from user device.
Policy:	5
Type:	Achievement
Action:	Collect browser and contact information
Agent:	System
Stakeholder:	User, System
Constraints:	Hardware permission granted
Obstacles:	Hardware permission not granted (General failure) Account validation failed (Contract failure Requirement 2.2)
Pre-condition:	Requirement 2.1: Allow users to login
Post-condition:	-
Sub-goals:	Requirement 5.6: Use synchronized contacts to suggest friends

Goal 3: User and system activities while using service:

Once the user has successfully logged into facebook, the user is free to perform operations on the service. The functionalities are listed according to their precedence. Since there

are a lot of functionalities associated with facebook, there are a lot of functional objectives, these objectives are listed below.

Requirement 3.1:	Create a new status
Policy:	1
Type:	Achievement
Action:	Create status
Agent:	User
Stakeholder:	User, System
Constraints:	User logged it
Obstacles:	Prevent duplicate statuses (General failure)
Pre-condition:	Requirement 2.1: Log into account
Post-condition:	Requirement 3.2: Collect status
	Requirement 3.3: Store status
Sub-goals:	Requirement 3.4: Delete created status
	Requirement 3.31: Privacy settings provided to the user

Requirement 3.2:	Collect created status
Policy:	1
Type:	Achievement
Action:	Collect status
Agent:	System
Stakeholder:	User, System
Constraints:	User creates a new status
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not create a status (Precedence failure)
Pre-condition:	Requirement 3.1: User creates a new status
Post-condition:	-
Sub-goals:	-

Requirement 3.3:	Store created status
Policy:	23
Type:	Achievement
Action:	Store status
Agent:	System
Stakeholder:	User, System
Constraints:	User logged it
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not create a status (Precedence failure)
Pre-condition:	Requirement 3.1: User creates a new status
Post-condition:	-
Sub-goals:	Requirement 3.5: Delete created status.

Requirement 3.4:	Modify existing status
Policy:	37
Type:	Achievement
Action:	Store status

Agent:	User
Stakeholder:	User, System
Constraints:	User logged it
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not create a status (Precedence failure)
Pre-condition:	Requirement 3.1: User creates a new status
Post-condition:	-
Sub-goals:	Requirement 3.31: Privacy settings provided to the user

Requirement 3.5:	Delete created status
Policy:	37
Type:	Achievement
Action:	Delete status
Agent:	User
Stakeholder:	User, System
Constraints:	Status exists in database
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not create a status (Precedence failure)
Pre-condition:	Requirement 3.1: User creates a new status
Post-condition:	-
Sub-goals:	-

Requirement 3.6:	Create new photo, video
Policy:	1
Type:	Achievement
Action:	Create photo, video
Agent:	User
Stakeholder:	User, System
Constraints:	User logged it
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
Pre-condition:	Requirement 2.1: Log into account
Post-condition:	Requirement 3.7: Collect photo, video
	Requirement 3.8: Store photo, video
Sub-goals:	Requirement 3.9: Delete created photo, video
	Requirement 3.31: Privacy settings provided to the user

Requirement 3.7:	Collect created photo, video
Policy:	1
Type:	Achievement
Action:	Collect photo, video
Agent:	System
Stakeholder:	User, System
Constraints:	User creates new photo or video
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not create a photo, video (Precedence failure)
Pre-condition:	Requirement 3.6: Create new photo, video
Post-condition:	-

Sub-goals:	-

Requirement 3.8:	Store created photo, video
Policy:	23
Type:	Achievement
Action:	Store photo, video
Agent:	System
Stakeholder:	User, System
Constraints:	User logged it
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not create a photo, video (Precedence failure)
Pre-condition:	Requirement 3.6: Create new photo, video
Post-condition:	-
Sub-goals:	Requirement 3.4: Delete created photo, video.

Requirement 3.9:	Delete created photo, video
Policy:	37
Type:	Achievement
Action:	Delete photo, video
Agent:	User
Stakeholder:	User, System
Constraints:	Photo(s) or video(s) exist in database
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not create a photo, video (Precedence failure)
Pre-condition:	Requirement 3.6: Create new photo, video
Post-condition:	-
Sub-goals:	-

Requirement 3.10:	User likes an object
Policy:	1
Type:	Achievement
Action:	Create like
Agent:	User
Stakeholder:	User, System
Constraints:	User logged it
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
Pre-condition:	Requirement 2.1: Log into account
Post-condition:	Requirement 3.11: Collect likes
	Requirement 3.12: Store likes
Sub-goals:	Requirement 3.13: Unlike object

Requirement 3.11:	Collect users like objects
Policy:	1
Type:	Achievement
Action:	Collect likes
Agent:	System
Stakeholder:	User, System

Constraints:	User likes on existing object
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not like and object (Precedence failure)
Pre-condition:	Requirement 3.10: User likes an object
Post-condition:	-
Sub-goals:	-

Requirement 3.12:	Store user likes on an object
Policy:	23
Type:	Achievement
Action:	Store user likes
Agent:	System
Stakeholder:	User, System
Constraints:	User logged in
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not like an object (Precedence failure)
Pre-condition:	Requirement 3.10: User likes an object
Post-condition:	-
Sub-goals:	Requirement 3.13: User dislikes a liked object.

Requirement 3.13:	User dislikes a liked object
Policy:	37
Type:	Achievement
Action:	Unlike object
Agent:	User
Stakeholder:	User, System
Constraints:	User has liked an object before disliking
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not like an object (Precedence failure)
Pre-condition:	Requirement 3.10: User likes an object.
Post-condition:	-
Sub-goals:	-

Requirement 3.14:	Send or create a new conversation
Policy:	1
Type:	Achievement
Action:	Create new conversation
Agent:	User
Stakeholder:	User, System
Constraints:	User logged it
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
Pre-condition:	Requirement 2.1: Log into account
Post-condition:	Requirement 3.15: Collect message
	Requirement 3.16: Store Messages
Sub-goals:	Requirement 3.17: Delete existing conversation

Requirement 3.15:	Collect conversations, sent or received

Policy:	1
Type:	Achievement
Action:	Collect conversations
Agent:	System
Stakeholder:	User, System
Constraints:	User creates or receives a new message
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not send or receive message (Precedence failure)
Pre-condition:	Requirement 3.14: Send a or create a new conversation
Post-condition:	-
Sub-goals:	-

Requirement 3.16:	Store conversations, sent or received
Policy:	23
Type:	Achievement
Action:	Store new conversations
Agent:	System
Stakeholder:	User, System
Constraints:	User creates or receives a new message
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not send or receive message (Precedence failure)
Pre-condition:	Requirement 3.14: Send a or create a new conversation
Post-condition:	-
Sub-goals:	-

Requirement 3.17:	Delete existing conversation.
Policy:	37
Type:	Achievement
Action:	Delete conversation
Agent:	User
Stakeholder:	User, System
Constraints:	User creates or receives a new message
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not send or receive message (Precedence failure)
Pre-condition:	Requirement 3.14: User sends or receives a new message
Post-condition:	-
Sub-goals:	-

Requirement 3.18:	Create a new check-in
Policy:	1
Type:	Achievement
Action:	Create check-in
Agent:	User
Stakeholder:	User, System
Constraints:	User logged it
Obstacles:	Location services turned off (Contract failure Requirement 2.11)
	Account validation failed (Contract failure Requirement 2.2)

Pre-condition:	Requirement 2.1: Allow users to login
Post-condition:	Requirement 3.19: Collect check-in
	Requirement 3.20: Store check-in
Sub-goals:	Requirement 3.21: Delete check-in
	Requirement 3.31: Privacy settings provided to the user

Requirement 3.19:	Collect new Check-in or tagged check-in
Policy:	1
Type:	Achievement
Action:	Collect check-in
Agent:	System
Stakeholder:	User, System
Constraints:	User creates a new check-in
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not create a check-in (General failure)
Pre-condition:	Requirement 3.18: User creates a new check-in
Post-condition:	-
Sub-goals:	-

Requirement 3.20:	Store user created check-in
Policy:	23
Type:	Achievement
Action:	Store check-in
Agent:	System
Stakeholder:	User, System
Constraints:	User creates a new check-in
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not create a check-in (General failure)
Pre-condition:	Requirement 3.18: User creates a new check-in
Post-condition:	-
Sub-goals:	Requirement 3.21: Delete user created check-ins

Requirement 3.21:	Delete user created check-in
Policy:	37
Type:	Achievement
Action:	Delete check-in
Agent:	User
Stakeholder:	User, System
Constraints:	User creates a new check-in
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not create a check-in (General failure)
Pre-condition:	Requirement 3.18: User creates a new check-in
Post-condition:	-
Sub-goals:	-

Requirement 3.22:	Add a friend to friend list
Policy:	1

Type:	Achievement
Action:	Add friend
Agent:	User
Stakeholder:	User, System
Constraints:	User logged it
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
Pre-condition:	Requirement 2.1: Allow users to login
Post-condition:	Requirement 3.23: Collect friend information
	Requirement 3.24: Store friend information
Sub-goals:	Requirement 3.25: Delete friend

Requirement 3.23:	Collect information of friend user added
Policy:	1
Type:	Achievement
Action:	Collect friend information
Agent:	System
Stakeholder:	User, System
Constraints:	User send a new friend request
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not add a new friend (General failure)
Pre-condition:	Requirement 3.22: User ads a new friend
Post-condition:	-
Sub-goals:	-

Requirement 3.24:	Store information of added friend
Policy:	23
Type:	Achievement
Action:	Store friend information
Agent:	System
Stakeholder:	User, System
Constraints:	User ads a new friend
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not add a new friend (General failure)
Pre-condition:	Requirement 3.22: User ads a new friend
Post-condition:	-
Sub-goals:	Requirement 3.25: User deletes a friend from friend list.

Requirement 3.25:	Delete friend from friend list
Policy:	37
Type:	Achievement
Action:	Delete friend
Agent:	User
Stakeholder:	User, System
Constraints:	User has friends in friend list
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not have friend in friend list (General failure)
Pre-condition:	Requirement 3.22: Add a friend to friend list

Post-condition:	Requirement 3.41: Store name and information of deleted friend
Sub-goals:	-

Requirement 3.26:	Tag friends on network
Policy:	9
Type:	Maintenance
Action:	Tag users
Agent:	User
Stakeholder:	User, System
Constraints:	There is content to tag a user
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
	User does not have tagged-user in friend list (General failure)
Pre-condition:	Requirement 3.22: User ads a friend
	Requirement 3.18: User creates a check-in
	Requirement 3.8: User creates a photo, video
	Requirement 3.1: Create a new status
Post-condition:	Requirement 3.27: Verify tag privileges
	Requirement 3.3: Store created status
	Requirement 3.8: Store created photo, video
	Requirement 3.16: Store conversations
	Requirement 3.20: Store created check-in
Sub-goals:	Requirement 3.28: Notify users of tag

Requirement 3.27:	Verify whether user can be tagged automatically
Policy:	9
Type:	Achievement
Action:	Verify tag
Agent:	System
Stakeholder:	User, System
Constraints:	User was tagged in a post
Obstacles:	User was not tagged (General failure)
Pre-condition:	Requirement 3.26: Allow users to tag other users
Post-condition:	Requirement 3.28: Tag approved
	Requirement 3.29: Tag disapproved
Sub-goals:	-

Requirement 3.28:	User approves or have automatic tagging available
Policy:	9
Type:	Achievement
Action:	Tag approved
Agent:	User
Stakeholder:	User, System
Constraints:	User was tagged in a post
Obstacles:	Verify if users can be tagged (General failure Requirement 3.27)
Pre-condition:	Requirement 3.26: Allow users to tag other users
Post-condition:	-
Sub-goals:	Requirement 3.30: Notify users of tag

Requirement 3.29:	Disapproves the tag
Policy:	9
Type:	Achievement
Action:	Tag disapproved
Agent:	User
Stakeholder:	User, System
Constraints:	User was tagged in a post
Obstacles:	User can be tagged automatically (General failure Requirement 3.27)
Pre-condition:	Requirement 3.27: User disables automatic tagging
Post-condition:	-
Sub-goals:	-

Requirement 3.30:	Notify when a tag is made
Policy:	9
Type:	Achievement
Action:	Notify users of tag
Agent:	System
Stakeholder:	User, System
Constraints:	User was tagged in a post
Obstacles:	User cancelled tag (Agent failure)
Pre-condition:	Requirement 2.26: Allow users to tag other users
Post-condition:	-
Sub-goals:	-

Requirement 3.31:	Privacy settings provided to the user
Policy:	14
Type:	Maintenance
Action:	Privacy settings available
Agent:	User
Stakeholder:	User, System
Constraints:	User is logged in and verified
Obstacles:	Account validation failed (Contract failure Requirement 2.2)
Pre-condition:	Requirement 2.1: User login
Post-condition:	Requirement 3.32: Share content with public Requirement 3.33: Share content with friends Requirement 3.34: Share content with custom list Requirement 3.35: Share content with friends of friends
Sub-goals:	-

Requirement 3.32:	Share content with public
Policy:	14
Type:	Maintenance
Action:	Share publically
Agent:	System
Stakeholder:	User, System

Constraints:	User sets privacy policy
Obstacles:	-
Pre-condition:	User sets privacy
Post-condition:	Requirement 3.36: Index user data on search engines Requirement 3.37: Make user data available on API
Sub-goals:	-

Requirement 3.33:	Share content with friends
Policy:	14
Type:	Maintenance
Action:	Share with friends
Agent:	System
Stakeholder:	User, System
Constraints:	User sets privacy policy
Obstacles:	-
Pre-condition:	User sets privacy
Post-condition:	Data shared with friends
Sub-goals:	-

Requirement 3.34:	Share content with custom list
Policy:	14
Type:	Maintenance
Action:	Share custom
Agent:	System
Stakeholder:	User, System
Constraints:	User sets privacy policy
Obstacles:	-
Pre-condition:	User sets privacy
Post-condition:	Data shared with custom list
Sub-goals:	-

Requirement 3.35:	Share content with friends of friend
Policy:	14
Type:	Maintenance
Action:	Share with friends of friend
Agent:	System
Stakeholder:	User, System
Constraints:	User sets privacy policy as public
Obstacles:	-
Pre-condition:	User sets privacy
Post-condition:	Data shared with friends of friend
Sub-goals:	-

Requirement 3.36:	Index content on search engines
Policy:	14
Type:	Maintenance
Action:	Share with search engines

Agent:	System
Stakeholder:	User, System
Constraints:	User sets privacy policy
Obstacles:	-
Pre-condition:	User sets privacy
Post-condition:	Data indexed on search engines
Sub-goals:	-

Requirement 3.37:	Allow API to access public data
Policy:	14
Type:	Maintenance
Action:	Share content on API
Agent:	System
Stakeholder:	User, System
Constraints:	User sets privacy policy as public
Obstacles:	-
Pre-condition:	User sets privacy
Post-condition:	Data indexed on search engines
Sub-goals:	-

Requirement 3.38:	Download data from facebook
Policy:	16
Type:	Achievement
Action:	Download data
Agent:	User
Stakeholder:	User, System
Constraints:	Data available to download
Obstacles:	Content deleted (General failure)
Pre-condition:	Requirement 2.1: User logged in
Post-condition:	Data downloaded
Sub-goals:	-

Requirement 3.39:	Store time and date of content creation
Policy:	1
Type:	Achievement
Action:	Store time and date
Agent:	System
Stakeholder:	User, System
Constraints:	New content created or modified
Obstacles:	Content not created or modified (General failure)
Pre-condition:	Create post, photo or videos.
Post-condition:	-
Sub-goals:	-

Requirement 3.40:	Ensure data availability by storing copies of user content
Policy:	37
Type:	Maintenance

Action:	Make copies of user data
Agent:	System
Stakeholder:	User, System
Constraints:	-
Obstacles:	-
Pre-condition:	User creates or modifies data
Post-condition:	Copies made
Sub-goals:	-

Goal 4: Purchasing activities performed by user on facebook:

A verified user on facebook may purchase over facebook in form of buying advertisement space, donating on facebook or buying gifts over facebook. The functionalities associated with this activity are listed below.

Requirement 4.1:	Provide purchasing options
Policy:	4
Type:	Maintenance
Action:	Financial transactions provided
Agent:	System
Stakeholder:	User, System
Constraints:	-
Obstacles:	User account not validated (General failure Requirement 2.2)
Pre-condition:	-
Post-condition:	-
Sub-goals:	Requirement 4.2: Allow users to donate, advertise and purchase gifts on facebook

Requirement 4.2:	Allow users to donate, advertise and purchase gifts on facebook
Policy:	4
Type:	Maintenance
Action:	Purchasing services available
Agent:	System
Stakeholder:	User, System
Constraints:	User is logged in and verified
Obstacles:	User account not validated (General failure Requirement 2.2)
Pre-condition:	-
Post-condition:	Require credit/debit card number from user
Sub-goals:	-

Requirement 4.3:	Provide credit/debit card number
Policy:	4
Type:	Achievement
Action:	Require credit/debit card number
Agent:	User
Stakeholder:	User, System
Constraints:	User makes a purchase over facebook

Obstacles:	User account not validated (General failure Requirement 2.2)
Pre-condition:	-
Post-condition:	Requirement 4.4: Verify payment information provided by user
	Requirement 4.5: Require shipping and billing address
Sub-goals:	-

Requirement 4.4:	Verify payment information provided by user
Policy:	4
Type:	Achievement
Action:	Verify payment
Agent:	System
Stakeholder:	User, System
Constraints:	User makes a purchase over facebook
Obstacles:	User account not validated (General failure Requirement 2.2)
Pre-condition:	Requirement 4.3: User provides credit/debit card number
Post-condition:	Requirement 4.5: Information validated
	Requirement 4.6: Information rejected
Sub-goals:	-

Requirement 4.5:	Credit/debit card number verified
Policy:	4
Type:	Achievement
Action:	Payment verified
Agent:	System
Stakeholder:	User, System
Constraints:	Information provided by user is correct
Obstacles:	Credit/debit card information rejected (Agent failure)
Pre-condition:	Requirement 4.2: User makes a purchase on facebook
Post-condition:	Requirement 4.7: Require shipping, billing address from user
Sub-goals:	Requirement 4.8: Collect credit/debit card number
	Requirement 4.9: Store credit/debit card number

Requirement 4.6:	Credit/debit card number invalid
Policy:	4
Type:	Achievement
Action:	Payment rejected
Agent:	System
Stakeholder:	User, System
Constraints:	User enters invalid credit/debit card number
Obstacles:	User account not validated (General failure Requirement 2.2)
Pre-condition:	Requirement 4.3: Provide credit/debit card number
Post-condition:	Payment declined
Sub-goals:	-

Requirement 4.7:	Enter shipping, billing address
Policy:	4
Type:	Achievement

Action:	Require shipping information
Agent:	User
Stakeholder:	User, System
Constraints:	Credit, debit card number verified
Obstacles:	Requirement 4.6: Credit/debit card number invalid
Pre-condition:	Requirement 4.5: Credit/debit card number verified
Post-condition:	Order confirmed
Sub-goals:	Requirement 4.10: Collect shipping, billing information
	Requirement 4.11: Store shipping, billing information

Requirement 4.8:	Collect credit/debit card number provided by user
Policy:	1
Type:	Achievement
Action:	Collect credit information
Agent:	System
Stakeholder:	User, System
Constraints:	User makes a purchase on facebook
Obstacles:	Requirement 4.6: Invalid credit/debit card number
Pre-condition:	Requirement 4.5: Credit/debit card number verified
Post-condition:	Credit/debit card number collected
Sub-goals:	-

Requirement 4.9:	Store credit/debit card number entered by user
Policy:	23
Type:	Achievement
Action:	Store credit/debit card number
Agent:	System
Stakeholder:	User, System
Constraints:	User makes a purchase on facebook
Obstacles:	Requirement 4.6: Invalid credit/debit card number
Pre-condition:	Requirement 4.5: Credit/debit card number verified
Post-condition:	Credit/debit card number stored
	Requirement 7.2: Encrypt credit/debit card number.
Sub-goals:	-

Requirement 4.10:	Collect shipping, billing information provided by user
Policy:	1
Type:	Achievement
Action:	Collect shipping information
Agent:	System
Stakeholder:	User, System
Constraints:	User makes a purchase on facebook
Obstacles:	Requirement 4.6: Invalid credit/debit card number
Pre-condition:	Requirement 4.7: Shipping and billing information entered
Post-condition:	Shipping, billing information collected
Sub-goals:	-

Requirement 4.11:	Store shipping, billing information provided by user
Policy:	23
Type:	Achievement
Action:	Store credit/debit card number
Agent:	System
Stakeholder:	User, System
Constraints:	User makes a purchase on facebook
Obstacles:	Requirement 4.6: Invalid credit/debit card number
Pre-condition:	Requirement 4.7: Shipping and billing information entered
Post-condition:	Shipping, billing information stored
Sub-goals:	-

Goal 5: Behind content creation on Facebook:

User can create modify and delete content over Facebook, however, there are a lot of activities SNS may perform 'behind the scenes'. Such activities are represented as functionalities in tables below.

Requirement 5.1:	Collect browsing patterns of user activities and time spent using the service
Policy:	1
Type:	Maintenance
Action:	Collect browsing information
Agent:	System
Stakeholder:	User, System
Constraints:	User is online
Obstacles:	-
Pre-condition:	Requirement 2.1: User login
Post-condition:	Information collected
Sub-goals:	-

Requirement 5.2:	Collect information in which user is tagged
Policy:	2
Type:	Achievement
Action:	Collect tagged information
Agent:	System
Stakeholder:	User, System
Constraints:	User is tagged in a post
Obstacles:	Requirement 3.29: User disapproves tag
Pre-condition:	User approves tag
Post-condition:	Collect information
Sub-goals:	-

Requirement 5.3:	Aggregate available pictures to suggest picture tags
Policy:	9
Type:	Achievement
Action:	Suggest picture tags

Agent:	System
Stakeholder:	User, System
Constraints:	Pictures available to perform aggregation
Obstacles:	Requirement 3.29: User disapproves tag
Pre-condition:	User approves tag
Post-condition:	Tag suggested
Sub-goals:	-

Requirement 5.4:	Use location to suggest nearby events to user
Policy:	10
Type:	Maintenance
Action:	Suggest events
Agent:	System
Stakeholder:	User, System
Constraints:	Location services available
Obstacles:	Requirement 2.11: User OPTS-OUT of location services
Pre-condition:	Users' location services available
Post-condition:	Suggest events
Sub-goals:	-

Requirement 5.5:	Use location services to suggest nearby places to user
Policy:	10
Type:	Maintenance
Action:	Suggest places
Agent:	System
Stakeholder:	User, System
Constraints:	Location services available
Obstacles:	Requirement 2.11: User OPTS-OUT of location services
Pre-condition:	Users' location services available
Post-condition:	Suggest places
Sub-goals:	-

Requirement 5.6:	Use synchronized contacts to suggest new friends
Policy:	10
Type:	Achievement
Action:	Suggest new networks
Agent:	System
Stakeholder:	User, System
Constraints:	Requirement 2.15: Synchronize contacts from user device
Obstacles:	Requirement 2.12: User disallows hardware access
Pre-condition:	Users' hardware access available
Post-condition:	Suggest friends
Sub-goals:	-

Requirement 5.7:	Transfer all available information to authorities
Policy:	25
Type:	Achievement

Action:	Transfer data to authorities
Agent:	System
Stakeholder:	User, System
Constraints:	User account available
Obstacles:	-
Pre-condition:	Authorities request user data
Post-condition:	Data transferred
Sub-goals:	-

Requirement 5.8:	Transfer data to partners, vendors and providers
Policy:	21
Type:	Achievement
Action:	Transfer data to partners
Agent:	System
Stakeholder:	User, System
Constraints:	User content available
Obstacles:	-
Pre-condition:	Partners request data
Post-condition:	Data transferred
Sub-goals:	-

Goal 6: Advertisement services on facebook:

Facebook from time to time may advertise on users' feed. Facebook may use collected information to display relevant ads or provide users with out of the context ads. Functionalities responsible for such activities are listed in table below.

Requirement 6.1:	Single sign on feature provided
Policy:	6
Type:	Maintenance
Action:	SSO functionality available
Agent:	System
Stakeholder:	Third party, System
Constraints:	-
Obstacles:	-
Pre-condition:	Services request SSO feature
Post-condition:	-
Sub-goals:	-

Requirement 6.2:	Advertisement and management service provided
Policy:	6
Type:	Maintenance
Action:	Advertisement services available
Agent:	System
Stakeholder:	Advertisers, Organization
Constraints:	-
Obstacles:	-

Pre-condition:	Advertisement services requested
Post-condition:	Advertisement services provided
Sub-goals:	-

Requirement 6.3:	Monitor users off service
Policy:	7
Type:	Maintenance
Action:	Monitor users
Agent:	System
Stakeholder:	User, system
Constraints:	-
Obstacles:	-
Pre-condition:	User uses third party service
Post-condition:	Browsing history tracked
Sub-goals:	Requirement 6.4: Collect browsing patterns

Requirement 6.4:	Collect browsing patterns of user off service
Policy:	1
Type:	Maintenance
Action:	Collect browsing data
Agent:	System
Stakeholder:	User, system
Constraints:	Users monitored
Obstacles:	Third party service does not use Facebook services (General failure)
Pre-condition:	Requirement 6.3: Monitor users off Facebook
Post-condition:	Browsing patterns collected.
	Requirement 6.5: Aggregate information to display relevant ads.
Sub-goals:	-

Requirement 6.5:	Aggregate available information to display relevant ads.
Policy:	12
Type:	Maintenance
Action:	Display ads
Agent:	System
Stakeholder:	User, system
Constraints:	Relevant information available
Obstacles:	-
Pre-condition:	User allows relevant advertisements
Post-condition:	Relative ads displayed
Sub-goals:	Requirement 6.6: Collect user activity on clicked ads

Requirement 6.6:	Collect user activity on clicked ads
Policy:	5
Type:	Maintenance
Action:	Collect advertisement activity
Agent:	System

Stakeholder:	User, system
Constraints:	Relevant ads displayed and clicked on
Obstacles:	Relevant advertisements not displayed.
Pre-condition:	Requirement 6.5: Aggregate available information to display relevant ads
Post-condition:	Requirement 6.7: Aggregate advertisement statistics
Sub-goals:	-

Requirement 6.7:	Aggregate statistics based on clicked ads.
Policy:	12
Type:	Achievement
Action:	Aggregate statistics.
Agent:	System
Stakeholder:	User, system
Constraints:	User clicked on ads.
Obstacles:	Aggregate information to display ads (Precedence failure Requirement 6.5)
Pre-condition:	Requirement 6.6: Collect user activity on clicked ads.
Post-condition:	Requirement 6.8: Aggregate information to hide PII.
Sub-goals:	Requirement 6.10: Receive browsing patterns and activity from third party services.

Requirement 6.8:	Aggregate advertisement statistics to hide PII
Policy:	12
Type:	Achievement
Action:	Hide PII
Agent:	System
Stakeholder:	User, system
Constraints:	Statistics gathered from displayed ads.
Obstacles:	Relevant advertisements not displayed.
Pre-condition:	Requirement 6.7: Aggregate statistics based on clicked ads.
Post-condition:	Requirement 6.9: Transfer advertisement statistics to advertisers.
Sub-goals:	-

Requirement 6.9:	Transfer advertisement statistics to advertisers.
Policy:	12
Type:	Achievement
Action:	Transfer statistics
Agent:	System
Stakeholder:	User, system
Constraints:	Relevant ads displayed on users' profile
Obstacles:	Statistics not aggregated (Requirement 6.8 precedence failure)
Pre-condition:	Requirement 6.7: Aggregate statistics based on clicked ads. Requirement 6.8: Aggregate statistics to hide PII.
Post-condition:	Statistics transferred.

Sub-goals:	Requirement 6.10: Receive browsing patterns from third party services

Requirement 6.10:	Receive browsing patterns from third party services.
Policy:	7
Type:	Maintenance
Action:	Receive statistics.
Agent:	System
Stakeholder:	User, system
Constraints:	-
Obstacles:	User does not use third party service
Pre-condition:	User uses third party service.
Post-condition:	Statistics received.
Sub-goals:	-

Requirement 6.11:	Improve marketing service by suggesting campaigns to user
Policy:	12
Type:	Achievement
Action:	Improve marketing
Agent:	System
Stakeholder:	User, system
Constraints:	User contact information available
Obstacles:	-
Pre-condition:	New marketing campaigns made available
Post-condition:	Requirement 6.12: Contact user
Sub-goals:	-

Requirement 6.12:	Contact user to offer new marketing campaigns.
Policy:	11
Type:	Achievement
Action:	Contact user
Agent:	System
Stakeholder:	User, system
Constraints:	New marketing campaigns.
Obstacles:	No new marketing campaigns available.
Pre-condition:	Requirement 6.11: Improve marketing campaigns.
Post-condition:	User contacted.
Sub-goals:	-

Goal 7: Usage of data:

Facebook can and will user data for a feature or to transfer information for financial benefits. Some of the highlighted functionalities are described in tables listed below.

Requirement 7.1:	Use available information to provide search features
Policy:	9
Type:	Maintenance

Action:	Use information for functionalities
Agent:	System
Stakeholder:	User, system
Constraints:	-
Obstacles:	-
Pre-condition:	Relevant information available
Post-condition:	-
Sub-goals:	-

Requirement 7.2:	Encrypt user data whenever data is created or modified.
Policy:	13
Type:	Maintenance
Action:	Encrypt data
Agent:	System
Stakeholder:	User, system
Constraints:	-
Obstacles:	-
Pre-condition:	User creates content
Post-condition:	Data encrypted
Sub-goals:	Requirement 7.3: Improve safety

Requirement 7.3:	Improve user safety
Policy:	11
Type:	Achievement
Action:	Improve safety
Agent:	System
Stakeholder:	User, system
Constraints:	-
Obstacles:	Data not encrypted (Requirement 7.2: Contract failure)
Pre-condition:	Requirement 7.2: Encrypt user data.
Post-condition:	-
Sub-goals:	-

Goal 8: Integrity and security:

Facebook deals with a lot of private user information. The information has to be secured efficiently and a few policies listed by facebook justify they are doing a lot to maintain integrity.

Requirement 8.1:	Monitor user transactions
Policy:	29
Type:	Maintenance
Action:	Monitor transactions
Agent:	System
Stakeholder:	User, system
Constraints:	User makes transactions

Obstacles:	Credit/debit card number invalid (Requirement 4.6: Contract failure)
Pre-condition:	Requirement 4.5: Transaction verified
Post-condition:	Transaction monitored
Sub-goals:	-

Requirement 8.2:	Monitor active friends of user
Policy:	31
Type:	Maintenance
Action:	Monitor users
Agent:	System
Stakeholder:	User, system
Constraints:	User online.
Obstacles:	Users offline (General failure)
Pre-condition:	Requirement 2.1: User login
Post-condition:	Display list of active friends.
Sub-goals:	-

Requirement 8.3:	Route traffic to improve service
Policy:	32
Type:	Maintenance
Action:	Improve performance
Agent:	System
Stakeholder:	User, system
Constraints:	-
Obstacles:	Location services disabled (Requirement 2.9: Contract failure)
Pre-condition:	Requirement 2.9: Location services available
Post-condition:	Improved performance
Sub-goals:	-

Requirement 8.4:	Report suspicious activity
Policy:	13
Type:	Achievement
Action:	Report activity
Agent:	User
Stakeholder:	User, system
Constraints:	-
Obstacles:	-
Pre-condition:	Content violates terms and services
Post-condition:	Requirement 8.5: Verify activity
Sub-goals:	-

Requirement 8.5:	Verify reported activity
Policy:	13
Type:	Achievement
Action:	Verify report
Agent:	System

Stakeholder:	User, system
Constraints:	Report submitted
Obstacles:	-
Pre-condition:	Requirement 8.4: User reports suspicious activity
Post-condition:	Requirement 8.6: Suspicious activity confirmed Requirement 8.7: Suspicious activity not detected
Sub-goals:	-

Requirement 8.6:	Suspicious activity confirmed.
Policy:	13
Type:	Achievement
Action:	Confirm report
Agent:	System
Stakeholder:	User, system
Constraints:	-
Obstacles:	-
Pre-condition:	Requirement 8.5: Verify reported activity
Post-condition:	Requirement 8.8: Disable account
Sub-goals:	-

Requirement 8.7:	Suspicious activity not detected
Policy:	13
Type:	Achievement
Action:	Deny report
Agent:	System
Stakeholder:	User, system
Constraints:	Activity not violating terms and policies
Obstacles:	-
Pre-condition:	Requirement 8.5: Verify reported activity
Post-condition:	-
Sub-goals:	-

Requirement 8.8:	Disable user account
Policy:	13
Type:	Achievement
Action:	Disable account
Agent:	System
Stakeholder:	User, system
Constraints:	Account reported of suspicious activity
Obstacles:	Suspicious activity not detected (Requirement 8.7: Contract failure)
Pre-condition:	Requirement 8.6: Suspicious activity confirmed
Post-condition:	-
Sub-goals:	-

Requirement 8.9:	Identify spammers and prevent them from using service
Policy:	33

Type:	Maintenance
Action:	Track spammers
Agent:	System
Stakeholder:	User, system
Constraints:	-
Obstacles:	-
Pre-condition:	User creates, shares a post.
Post-condition:	Requirement 8.10:Prevent from using service
Sub-goals:	-

Requirement 8.10:	Monitor off service usage to track underage users
Policy:	34
Type:	Maintenance
Action:	Monitor underage users
Agent:	System
Stakeholder:	User, system
Constraints:	-
Obstacles:	-
Pre-condition:	Underage users using service
Post-condition:	Requirement 8.10: Prevent from using service
Sub-goals:	-

Requirement 8.11:	Prevent users from using service
Policy:	34
Type:	Achievement
Action:	Prevent usage
Agent:	System
Stakeholder:	User, system
Constraints:	-
Obstacles:	-
Pre-condition:	Requirement 8.9: Identify spammers and prevent them from using service Requirement 8.10: Monitor off service usage to track underage users
Post-condition:	Users prevented from using service
Sub-goals:	-

Requirement 8.12:	Discourage users from posting spam
Policy:	38
Type:	Achievement
Action:	Advise against spam
Agent:	System
Stakeholder:	User, system
Constraints:	-
Obstacles:	-
Pre-condition:	Requirement 2.1: User login
Post-condition:	-

Sub-goals:	-

Requirement 8.13:	Discourage users from collecting data
Policy:	38
Type:	Achievement
Action:	Advise against data collection
Agent:	System
Stakeholder:	User, system
Constraints:	-
Obstacles:	-
Pre-condition:	Requirement 2.1: User login
Post-condition:	-
Sub-goals:	-

Requirement 8.14:	Discourage users from harassing other users
Policy:	38
Type:	Achievement
Action:	Advise against harassment
Agent:	System
Stakeholder:	User, system
Constraints:	-
Obstacles:	-
Pre-condition:	Requirement 2.1: User login
Post-condition:	-
Sub-goals:	-

Requirement 8.15:	Discourage users from violating terms and services.
Policy:	38
Type:	Achievement
Action:	Advise against violation of services
Agent:	System
Stakeholder:	User, system
Constraints:	-
Obstacles:	-
Pre-condition:	Requirement 2.1: User login
Post-condition:	-
Sub-goals:	-

Requirement 8.16:	Identify access from public computer
Policy:	38
Type:	Achievement
Action:	Identify access
Agent:	System
Stakeholder:	User, system
Constraints:	User logs into facebook
Obstacles:	-
Pre-condition:	Requirement 2.1: User login

Post-condition:	Requirement 8.17: Advise against saving credentials
Sub-goals:	-

Requirement 8.17:	Discourage users from saving credentials on public computers
Policy:	38
Type:	Maintenance
Action:	Advise against saving credentials
Agent:	System
Stakeholder:	User, system
Constraints:	Environment is accessed via public computer
Obstacles:	User not advised (General failure)
Pre-condition:	Requirement 8.16: Identify access from public computers.
Post-condition:	-
Sub-goals:	-

Goal 9: Facebook API:

Facebook API provides developers with a platform to connect their applications with facebook. Which also provides access to SSO feature, using that, users can use multiple services using facebook authentication. The authentication also grants developers access to public user data, upon consent, developers may also be able to access private data. Functionalities associated with Facebook API are listed in table below.

Requirement 9.1:	Access publically available data
Policy:	17
Type:	Achievement
Action:	Access public profile
Agent:	Developer.
Stakeholder:	Developer, User
Constraints:	Public profile requested.
Obstacles:	-
Pre-condition:	User uses third party application
Post-condition:	Grant access to public profile
Sub-goals:	-

Requirement 9.2:	Access to private data provided
Policy:	39
Type:	Maintenance
Action:	Access private data
Agent:	System
Stakeholder:	Developer, User
Constraints:	Developer requests to access private data.
Obstacles:	-
Pre-condition:	Developer requests private data.
Post-condition:	Requirement 9.3: Review application
Sub-goals:	-

Requirement 9.3:	Review application that requests private data.
Policy:	39
Type:	Achievement
Action:	Review application
Agent:	System
Stakeholder:	Developer, System
Constraints:	-
Obstacles:	-
Pre-condition:	Requirement 9.2: Access to private data provided
Post-condition:	Requirement 9.4: Approve application Requirement 9.5: Disapprove application
Sub-goals:	-

Requirement 9.4:	Grant developer access to private user data
Policy:	39
Type:	Achievement
Action:	Approve application
Agent:	System
Stakeholder:	Developer, System
Constraints:	-
Obstacles:	Application review failed (Requirement 9.3: Contract failure)
Pre-condition:	Requirement 9.3: Review application that requests private data.
Post-condition:	Requirement 9.6: Acquire user consent
Sub-goals:	-

Requirement 9.5:	Disallow developers from accessing user data
Policy:	39
Type:	Achievement
Action:	Disapprove application
Agent:	System
Stakeholder:	User, system
Constraints:	-
Obstacles:	-
Pre-condition:	Requirement 9.3: Review application that requests private data.
Post-condition:	-
Sub-goals:	-

Requirement 9.6:	Acquire user consent before granting developers access
Policy:	39
Type:	Achievement
Action:	Acquire consent
Agent:	System
Stakeholder:	Developer, system
Constraints:	-
Obstacles:	-
Pre-condition:	Requirement 9.4: Grant developer access to private user data.
Post-condition:	Requirement 9.7: User accepts consent

	Requirement 9.8: User rejects consent
Sub-goals:	-

Requirement 9.7:	User grants developer access to private data
Policy:	39
Type:	Achievement
Action:	User accepts consent
Agent:	User
Stakeholder:	Developer, User
Constraints:	-
Obstacles:	-
Pre-condition:	Requirement 9.4: Grant developer access to private user data.
Post-condition:	-
Sub-goals:	Requirement 9.9: Share game activities Requirement 9.10: Share user photos Requirement 9.11: Share user comments Requirement 9.12: Share messages Requirement 9.13: Share events Requirement 9.14: Share friend list Requirement 9.15: Share user likes Requirement 9.16: Share user posts

Requirement 9.8:	User does not grant developer access to data
Policy:	39
Type:	Achievement
Action:	Reject consent
Agent:	User
Stakeholder:	Developer, User
Constraints:	-
Obstacles:	-
Pre-condition:	Requirement 9.4: Grant developer access to private user data.
Post-condition:	-
Sub-goals:	-

Requirement 9.9:	Share user game activities with developers
Policy:	40
Type:	Maintenance
Action:	Share game activities
Agent:	System
Stakeholder:	Developer, User
Constraints:	-
Obstacles:	User does not grant access to private data (Requirement 9.7: Contract failure)
Pre-condition:	Requirement 9.3: Review application that requests private data. Requirement 9.7: User accepts consent.
Post-condition:	Reacquire user consent
Sub-goals:	-

Requirement 9.10:	Share user photos with developers
Policy:	40
Type:	Maintenance
Action:	Share user photos
Agent:	System
Stakeholder:	Developer, User
Constraints:	-
Obstacles:	User does not grant access to private data (Requirement 9.7: Contract failure)
Pre-condition:	Requirement 9.3: Review application that requests private data. Requirement 9.7: User accepts consent.
Post-condition:	Reacquire user consent
Sub-goals:	-

Requirement 9.11:	Share user comments with developers
Policy:	40
Type:	Maintenance
Action:	Share comments
Agent:	System
Stakeholder:	Developer, User
Constraints:	-
Obstacles:	User does not grant access to private data (Requirement 9.7: Contract failure)
Pre-condition:	Requirement 9.3: Review application that requests private data. Requirement 9.7 User accepts consent.
Post-condition:	Reacquire user consent
Sub-goals:	-

Requirement 9.12:	Share messages sent to a group with developers
Policy:	40
Type:	Maintenance
Action:	Share messages
Agent:	System
Stakeholder:	Developer, User
Constraints:	-
Obstacles:	User does not grant access to private data (Requirement 9.7: Contract failure)
Pre-condition:	Requirement 9.3: Review application that requests private data. Requirement 9.7: User accepts consent.
Post-condition:	Reacquire user consent
Sub-goals:	-

Requirement 9.13:	Share user events with developers
Policy:	40
Type:	Maintenance
Action:	Share events

Agent:	System
Stakeholder:	Developer, User
Constraints:	-
Obstacles:	User does not grant access to private data (Requirement 9.7: Contract failure)
Pre-condition:	Requirement 9.3: Review application that requests private data. Requirement 9.7: User accepts consent.
Post-condition:	Reacquire user consent
Sub-goals:	-

Requirement 9.14:	Share user friend list with developers
Policy:	40
Type:	Maintenance
Action:	Share friend list
Agent:	System
Stakeholder:	Developer, User
Constraints:	-
Obstacles:	User does not grant access to private data (Requirement 9.7: Contract failure)
Pre-condition:	Requirement 9.3: Review application that requests private data. Requirement 9.7: User accepts consent.
Post-condition:	Reacquire user consent
Sub-goals:	-

Requirement 9.15:	Share content from user groups with developers
Policy:	40
Type:	Maintenance
Action:	Share group content
Agent:	System
Stakeholder:	Developer, User
Constraints:	-
Obstacles:	User does not grant access to private data (Requirement 9.7: Contract failure)
Pre-condition:	Requirement 9.3: Review application that requests private data. Requirement 9.7: User accepts consent.
Post-condition:	Reacquire user consent
Sub-goals:	-

Requirement 9.16:	Share user likes with developers
Policy:	40
Type:	Maintenance
Action:	Share likes
Agent:	System
Stakeholder:	Developer, User
Constraints:	-
Obstacles:	User does not grant access to private data (Requirement 9.7: Contract failure)

Pre-condition:	Requirement 9.3: Review application that requests private data. Requirement 9.7: User accepts consent.
Post-condition:	Reacquire user consent
Sub-goals:	-

Requirement 9.17:	Share user posts with developers
Policy:	40
Type:	Maintenance
Action:	Share posts
Agent:	System
Stakeholder:	Developer, User
Constraints:	-
Obstacles:	User does not grant access to private data (Requirement 9.7: Contract failure)
Pre-condition:	Requirement 9.3: Review application that requests private data. Requirement 9.7: User accepts consent.
Post-condition:	Reacquire user consent
Sub-goals:	-

Requirement 9.18:	Reacquire user consent with rights to object
Policy:	40
Type:	Maintenance
Action:	Require rights
Agent:	Developer
Stakeholder:	Developer, User
Constraints:	-
Obstacles:	User does not grant access to private data (Requirement 9.7: Contract failure)
Pre-condition:	Requirement 9.7: User accepts consent.
Post-condition:	Requirement 9.19: Accept consent Requirement 9.20: Reject consent
Sub-goals:	-

Requirement 9.19:	Allow developers the rights to object
Policy:	40
Type:	Achievement
Action:	Share requested data
Agent:	User
Stakeholder:	Developer, User
Constraints:	-
Obstacles:	User does not grant access to private data (Requirement 9.18: Contract failure)
Pre-condition:	Developers access new private data.
Post-condition:	Allow developers to access content.
Sub-goals:	-

Requirement 9.20:	Disallow developers from accessing user data

Policy:	40
Type:	Achievement
Action:	Reject consent
Agent:	User
Stakeholder:	Developer, User
Constraints:	-
Obstacles:	-
Pre-condition:	Requirement 9.18: Require consent from user
Post-condition:	Access not granted
Sub-goals:	-

Goal 10: Data management practices:

User must be allowed to control how data is controlled. For this, user is allowed to perform several actions to control their data. There are a few activities happening at the back-end as well, which are automated. These functionalities are listed in tables below.

Requirement 10.1:	Allow users to delete their account
Policy:	23
Type:	Achievement
Action:	Delete account
Agent:	User
Stakeholder:	System, User
Constraints:	-
Obstacles:	-
Pre-condition:	Requirement 1.2: User creates an account
Post-condition:	Delete account and data associated with it Requirement 10.2: Keep data of deleted account
Sub-goals:	-

Requirement 10.2:	Keep data of deleted account
Policy:	23
Type:	Achievement
Action:	Retain data
Agent:	System
Stakeholder:	System, User
Constraints:	-
Obstacles:	-
Pre-condition:	Requirement 10.1: User deletes account
Post-condition:	Make data invisible for other users
Sub-goals:	-

Uncovered goals:

Goals may be uncovered after analyzing vulnerabilities. Some vulnerabilities may exist to provide some security features to the user. Such goals (after evaluation of vulnerabilities) are listed in tables below.

Requirement 2.16:	Log login activity to help against unauthorized access.
Policy:	28
Type:	Achievement
Action:	Log activity
Agent:	System
Stakeholder:	System, User
Constraints:	User logs into account
Obstacles:	-
Pre-condition:	Requirement 2.4: Monitor login activity of active account
Post-condition:	Requirement 2.17: Notify users of suspicious activity
Sub-goals:	-

Requirement 2.17:	Notify users of suspicious login activity
Policy:	28
Type:	Achievement
Action:	Notify suspicious login
Agent:	System
Stakeholder:	System, User
Constraints:	-
Obstacles:	-
Pre-condition:	Requirement 2.14: Suspicious login activity detected
Post-condition:	-
Sub-goals:	-

Requirement 3.41:	Store name and information of deleted friend
Policy:	37
Type:	Achievement
Action:	Store deleted friend information
Agent:	System
Stakeholder:	System, User
Constraints:	Friend is deleted by user
Obstacles:	Friend not deleted (General failure)
Pre-condition:	Requirement 3.25: User deletes a friend
Post-condition:	-
Sub-goals:	-

Appendix C

Privacy vulnerability interview

An interview to determine what are the actual vulnerabilities in a social networking system

1. **Do you use social networking service, Facebook ?**
   Mark only one oval.
   - ◯ Yes
   - ◯ No

2. **How often would you say that you use facebook?**
   Mark only one oval.
   - ◯ Daily
   - ◯ Once or twice a week
   - ◯ Once or twice a month
   - ◯ Other: .....

3. **What do you usually use facebook for ?**
   Mark only one oval.
   - ◯ Expanding network
   - ◯ Communication tool
   - ◯ Sharing pictures
   - ◯ Sharing statuses and comments
   - ◯ Other: .....

4. **Facebook may track your location, do you consider it a privacy violation ?**
   Mark only one oval.
   - ◯ Yes
   - ◯ No

5. **Location monitoring may be turned off, do you know how to do that?**

   .....

6. **Facebook may monitor usage activity on and off Facebook. Do you consider it a privacy vulnerability ?**
   Mark only one oval.
   - ◯ Yes
   - ◯ No

7. **Facebook may store information related to advertisements, i.e. when you clicked an ad, which ad you clicked and at what time. Do you consider it a privacy violation ?**
   Mark only one oval.
   - Yes
   - No

8. **When you browse internet, facebook may monitor cookies to determine which websites you visited. `this helps Facebook to display 'relevant' ads, do you consider it a privacy vulnerability ?**
   Mark only one oval.
   - Yes
   - No

9. **Facebook may synchronize contacts from your mobile device, this helps them to find you new 'friends' on facebook. Do you consider it a privacy vulnerability ?**
   Mark only one oval.
   - Yes
   - No

10. **Facebook may use your pictures to create a database for their facial recognition system. This offers features such as automatic picture tagging. Do you think of it as a privacy vulnerability ?**
    Mark only one oval.
    - Yes
    - No

11. **For those who display phone numbers can be searched using phone numbers on facebook, do you consider that as a privacy vulnerability ?**
    Mark only one oval.
    - Yes
    - No

12. **Facebook may transfer your data to partner companies, do you consider it a privacy vulnerability ?**
    Mark only one oval.
    - Yes
    - No

13. **Facebook stores a list of IP addresses used to access account, do you think of it as a privacy vulnerability ?**
    Mark only one oval.
    - Yes
    - No

14. **Developers may access your profile data, public and/or private (upon valid consent of-course) do you consider it a privacy violation ?**
Mark only one oval.

- Yes
- No

15. **Other users may download your information and may share it as their own, do you consider it a privacy violation**
Mark only one oval.

- Yes
- No

16. **Rate these from 1-5, 1 being not so personal information 5 being personal information**
Mark only one oval per row.

	1	2	3	4	5
Photos					
Email address					
Phone number					
Status					
Comment					
Likes					
Videos					
Friend list					
Events					
Credit/debit card number					

17. **Rate following from 1 - 5, 1 being not a privacy violation, 5 being a privacy violation**
Mark only one oval per row.

	1	2	3	4	5
Location monitoring					
Indirect data collection					
Searching with private information					
Data aggregation					
Monitoring browsing data					
Data transmission					
Monitoring					
Aggregation					
Storage					
Transfer					
Collection					
Personalization					

18. **Under what circumstances would you feel location monitoring is appropriate ?**

.....

19. **Under what circumstances do you feel indirect data collection, such as saving contacts from your device is appropriate ?**

.....

20. **Would you rather set all facebook privacy settings manually or have facebook set it for you in most private way ?**

Mark only one oval.

- ◯ Let facebook set it
- ◯ Set it yourself

21. **Information storage is necessary to provide features on Facebook, once the account is deleted, all instance of data must be deleted. However, Facebook may make copies of data and it may take some time before all instances are deleted. Do you consider it a privacy violation?**

Mark only one oval.

- ◯ Yes
- ◯ No

22. **Messages you send, receive or delete may be saved by Facebook. Do you consider it a privacy violation ?**

Mark only one oval.

- ◯ Yes
- ◯ No

23. **Data management process of a typical social networking service include data collection, data storage, data aggregation and data retrieval. What are your insecurities related to these activities?**

.....

.....

.....

.....

.....

24. **Do you have your phone number associated with your account ?**

Mark only one oval.

- ◯ Yes
- ◯ No

25. **Is your phone number private or public ?**

Mark only one oval.

- ◯ Private
- ◯ Public
- ◯ Dont know

26. **Are posts you make private, public or defined custom?**
Mark only one oval.

- Private
- Public
- Custom
- Dont know

27. **Is your email address private, public or custom ?**
Mark only one oval.

- Private
- Public
- Custom
- Other

28. **Is tag review feature enabled on your profile ?**
Mark only one oval.

- Yes
- No
- Dont know

29. **is ads based on your use of websites and apps enabled ?**
Mark only one oval.

- Yes
- No
- Dont know

30. **is your "Ads with my social actions" enabled ?**
Mark only one oval.

- Yes
- Know
- Dont know